

## A MODULAR APPROACH TO CUBIC THUE-MAHLER EQUATIONS

DOHYEONG KIM

ABSTRACT. Let  $h(x, y)$  be a non-degenerate binary cubic form with integral coefficients, and let  $S$  be an arbitrary finite set of prime numbers. By a classical theorem of Mahler, there are only finitely many pairs of relatively prime integers  $x, y$  such that  $h(x, y)$  is an  $S$ -unit. In the present paper, we reverse a well-known argument, which seems to go back to Shafarevich, and use the modularity of elliptic curves over  $\mathbb{Q}$  to give upper bounds for the number of solutions of such a Thue-Mahler equation. In addition, our methods give an effective method for determining all solutions, and we use Cremona’s Elliptic Curve Database to give a wide range of numerical examples.

### CONTENTS

1.	Introduction	1435
2.	Definition of $\kappa$ and its properties	1438
3.	Defining equations for the fibres of $\kappa$	1441
4.	Main theorems	1446
5.	Algorithmic aspects	1448
6.	Numerical examples	1449
7.	Comparison with the work of Tzanakis and de Weger	1455
8.	Generalised Ramanujan-Nagell equations	1456
	Acknowledgements	1470
	References	1470

### 1. INTRODUCTION

Let  $h(x, y)$  be a non-degenerate cubic form with integer coefficients, and let  $S$  be a finite set consisting of  $s$  distinct prime numbers, say  $p_1, p_2, \dots, p_s$ . Then the Thue-Mahler equation

$$(1.1) \quad h(x, y) = \pm \prod_{i=1}^s p_i^{e_i}$$

has finitely many solutions among relatively prime integers  $x, y$  and non-negative integers  $e_1, e_2, \dots, e_s$ . In geometric terms, if we denote by  $\mathbb{Z}_S$  the ring of  $S$ -integers, and by  $Y$  the affine variety defined as the complement of zeros of  $h(x, y)$  in a projective line, then the solutions of the above Thue-Mahler equation, modulo the identification of  $(x, y)$  and  $(-x, -y)$ , bijectively correspond to the elements of  $Y(\mathbb{Z}_S)$ .

---

Received by the editor June 9, 2015 and, in revised form, November 27, 2015.  
 2010 *Mathematics Subject Classification*. Primary 11D59, 11F11, 11Y50.

©2016 American Mathematical Society

Mahler gave an ineffective proof of the finiteness of  $Y(\mathbb{Z}_S)$ , and Coates [5], [6], [7] later obtained an effective proof of the finiteness of  $Y(\mathbb{Z}_S)$  using Baker's estimate of linear forms in logarithms together with its  $p$ -adic analogues. However, explicit determination of  $Y(\mathbb{Z}_S)$  based on Baker's method is often practically impossible due to the astronomical size of the resulting upper bound for the height of a putative solution  $t \in Y(\mathbb{Z}_S)$ .

The aim of the current article is to present a new approach to Thue-Mahler equations. In order to compute  $Y(\mathbb{Z}_S)$ , we design a descent procedure, which mimics the Kummer homomorphism for rational points on elliptic curves. More precisely, we will construct a natural map

$$(1.2) \quad \begin{aligned} \kappa: Y(\mathbb{Z}_S) &\longrightarrow \{\text{elliptic curves over } \mathbb{Q} \text{ up to } \mathbb{Q}\text{-isomorphism}\} \\ t &\longmapsto X_t \end{aligned}$$

which associates an elliptic curve  $X_t$  to an unknown solution  $t \in Y(\mathbb{Z}_S)$ , and study local properties of  $X_t$ . In particular, we will show that  $X_t$  has good reduction outside  $S$ , the discriminant of  $h(x, y)$ , that is, outside the primes dividing this discriminant, and 2. We note that in the current article, elliptic curves and isomorphisms between them will be defined over  $\mathbb{Q}$ . The aforementioned knowledge about the reduction types of  $X_t$  allows one to compute, without knowing elements of  $Y(\mathbb{Z}_S)$ , a finite set of isomorphism classes of elliptic curves which contains the image of  $\kappa$ . On the other hand, for an elliptic curve  $E$ , we will show that  $\kappa^{-1}(E)$  is naturally a zero dimensional algebraic variety defined by explicit polynomials with rational coefficients, whose  $\mathbb{Q}$ -points correspond to  $t \in Y(\mathbb{Z}_S)$  equipped with an isomorphism from  $X_t$  to  $E$ . In particular, one can numerically compute  $\kappa^{-1}(E)$  from the coefficients of a Weierstrass equation for  $E$ .

Existence of such a map  $\kappa$  first allows us to bound the cardinality of  $Y(\mathbb{Z}_S)$  from above, in terms of the number of elliptic curves whose conductor belongs to a finite list of integers, where the list of possible conductors is obtained from the coefficients of  $h(x, y)$  and  $S$ . The number of such elliptic curves can be bounded from above either using the work [4] of Brumer and Silverman or the modularity of elliptic curves. The former has better asymptotics, while the latter provides a practical algorithm.

**Theorem 1.1.** *Let  $S$  be a finite set of primes containing 2 and prime divisors of the discriminant of  $h(x, y)$ . Let  $G(S)$  be the number of isomorphism classes of elliptic curves which have good reduction outside  $S$ . Then we have*

$$(1.3) \quad |Y(\mathbb{Z}_S)| \leq |\text{Aut}_{\mathbb{Q}}(Y)| \times G(S).$$

Combining it with an upper bound for  $G(S)$ , due to Brumer and Silverman, we have for every  $\varepsilon > 0$ ,

$$(1.4) \quad |Y(\mathbb{Z}_S)| \leq |\text{Aut}_{\mathbb{Q}}(Y)| \times k_2 M^{\frac{1}{2} + \varepsilon}$$

where  $M$  is the product of all prime numbers in  $S$ , and  $k_2$  is a constant depending on  $\varepsilon$ .

In fact, one can identify  $\text{Aut}_{\mathbb{Q}}(Y)$  with a subgroup of the symmetric group acting on zeros of  $h(x, y)$ , so it has at most six elements.

We would like to stress that our proof is manifestly constructive, which ultimately relies on the modularity of elliptic curves defined over the rational numbers. More precisely, we give an explicit characterisation of the fibres of  $\kappa$  which allows us to

compute  $Y(\mathbb{Z}_S)$  from  $\kappa(Y(\mathbb{Z}_S))$ , and the modularity of elliptic curves provides a constructive finiteness of  $\kappa(Y(\mathbb{Z}_S))$ . In order to show that our approach to compute  $Y(\mathbb{Z}_S)$  works in practice, we append the tables with the complete sets of solutions of the following equations:

(1.5)

$h(x, y)$	$S$	Table
$x(x - y)y$	$\{2, 7, 11, 13\}$	8.1
$x(x - y)y$	$\{2, 3, 431\}$	8.2
$x(x - y)y$	$\{2, 3, 5, 53\}$	8.3
$(x^2 + 7y^2)y$	$\{2, 3, 5, 7\}$	8.4
$(x^2 + 7y^2)y$	$\{2, 7, 11, 13\}$	8.5
$(x^2 + 3y^2)y$	$\{2, 3, 11\}$	8.6
$2(x^2 + y^2)y$	$\{2, 3, 7, 11\}$	8.7
$(x^2 + y^2)y$	$\{2, 5, 13\}$	8.8
$(x^2 - 2y^2)y$	$\{2, 7, 29\}$	8.9
$(x^2 - 2y^2)y$	$\{2, 7, 29\}$	8.10
$(x^2 - 3y^2)y$	$\{2, 5, 7, 11\}$	8.11
$(x^2 - 7y^2)y$	$\{2, 3, 7, 11\}$	8.12
$x^3 - x^2y - 4xy^2 - y^3$	$\{2, 5, 13\}$	8.13
$x^3 - x^2y - 2xy^2 - 2y^3$	$\{2, 5, 19\}$	8.14
$x^3 + y^3$	$\{2, 3, 5\}$	8.15
$x^3 + 2y^3$	$\{2, 3, 5\}$	8.16
$x^3 - y^3$	$\{2, 3, 5\}$	8.17
$x^3 - 2y^3$	$\{2, 3, 5\}$	8.18

Note that we omitted the trivial solution  $h(1, 0) = 1$  in the appended tables, and that Table 8.3 had to be abbreviated due to a large number of solutions.

The choices of  $h(x, y)$  and  $S$  in (1.5) had to be restricted according to our computational capability, and the choices are made to show the flexibility that we have. The main restriction comes from one’s ability to find the  $c_4$  and  $c_6$  invariants of all elliptic curves whose conductor divides the worst possible conductor given in Proposition 2.1. Other computational difficulties are negligible. Computational issues are further discussed in Section 7.

When we computed the solutions of the equations listed above, we exploited Cremona’s Elliptic Curve Database, from which we read the coefficients of elliptic curves with a specified conductor. After that, we compute  $\kappa^{-1}(E)$  for each curve  $E$  read from the database. Of course, it is a highly non-trivial task to establish a complete list of isomorphism classes of elliptic curves of a specified conductor, and we are outsourcing this job to Cremona. We note that this job is computationally infeasible without modularity, and even with modularity it takes significant further efforts to obtain a practically efficient algorithm. Nevertheless, the absence of modularity is the main theoretical and practical obstacle to generalising our method to number fields. Once we have the coefficients of the necessary elliptic curves, then it takes no more than 20 seconds to generate each of the tables listed above.

The spectacular resolution of Fermat’s Last Theorem by means of modular methods as well as [1], [2], [3] and [9] uses the level lowering argument in a crucial way, which allows one to produce an obstruction to the existence of a solution by showing that a particular space of modular forms is zero dimensional. In contrast, we will be using the modularity theorem in order to produce a complete set of solutions for a

given Thue-Mahler equation, without an a priori guess on the number of solutions. In particular, we do not use any form of level lowering.

We outline the contents of the paper. In Section 2, we define  $\kappa$  and study basic properties of the elliptic curve  $X_t$  associated to  $t \in Y(\mathbb{Z}_S)$ . In Section 3, we study  $\kappa^{-1}(E)$  for an elliptic curve  $E$  given in terms of a Weierstrass equation. In Section 4, we prove the main theorem on the upper bound of the cardinality of  $Y(\mathbb{Z}_S)$  and compare our upper bound with Evertse's upper bound. The proof is manifestly constructive, and it provides an algorithm to determine  $Y(\mathbb{Z}_S)$ . We discuss the algorithmic aspect in Section 5. In Section 6, we explain how the algorithm is implemented in the computer algebra package and discuss its performance. We also list the cardinalities of  $Y(\mathbb{Z}_S)$  as we vary  $S$ . In Section 7, we recall the work of Tzanakis and de Weger, which proposed, based on Baker's method and further optimisations, a practical algorithm for Thue-Mahler equations, and we compare the natures of the two approaches. In Section 8, we specialise  $h(x, y)$  in order to explain the connection to generalised Ramanujan-Nagell equations. Some particular generalised Ramanujan-Nagell equations are solved, from which we observe a pattern in the distribution of the cardinality of  $Y(\mathbb{Z}_S)$  as  $S$  varies.

## 2. DEFINITION OF $\kappa$ AND ITS PROPERTIES

Consider a binary cubic form

$$(2.1) \quad h(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$$

with relatively prime integer coefficients. We assume that the discriminant

$$(2.2) \quad \delta = 3b^2c^2 + 6abcd - 4b^3d - 4ac^3 - a^2d^2$$

of  $h(x, y)$  is non-zero or equivalently that  $h(x, y)$  has three projectively non-equivalent zeros over an extension of  $\mathbb{Q}$ .

Let  $\mathbb{P}_{xy}^1$  be the projective line with homogeneous coordinates  $x$  and  $y$ . Let  $Z$  be the subscheme of  $\mathbb{P}_{xy}^1$  defined by  $h(x, y) = 0$ , and let  $Y$  be the complement

$$(2.3) \quad Y = \mathbb{P}^1 - Z,$$

which we view as an affine variety embedded in  $\mathbb{P}_{xy}^1$ . In particular, a point  $t$  in  $Y(R)$  for some ring  $R$  will be represented as a pair  $(x_t : y_t) \in \mathbb{P}^1(R)$  such that  $h(x_t, y_t)$  is a unit in  $R$ .

The aim of this section is to introduce the map  $\kappa$  which associates an elliptic curve to a point in  $Y(R)$  and to study its basic properties. We will first construct a generically smooth map from some affine scheme  $X$  to  $Y$ , and the elliptic curve associated to a point from  $Y$  will be the fibre of the point under this map. The associated elliptic curve is naturally equipped with additional structures, which we will analyse in this section.

**2.1. Coordinates of  $Y$ .** Our definition of  $Y$  as an open subscheme of  $\mathbb{P}_{xy}^1$  endows  $Y$  with homogeneous coordinates  $x$  and  $y$ , but we would like to introduce another coordinate  $\epsilon$  of  $Y$ , which makes our later discussion simpler. Consider  $\tilde{Y} \subset \mathbb{A}_{xy\epsilon}^3$ , defined by

$$(2.4) \quad \tilde{Y}: h(x, y)\epsilon = 1$$

where  $h(x, y)$  is the defining equation of  $Z = \mathbb{P}^1 - Y$ . Let  $\mathbb{G}_m$  act on  $\mathbb{A}^3_{xy\epsilon}$  with weight 1, 1, and  $-3$ . That is to say, for any ring  $R$ ,  $\lambda \in R^\times$ , and  $(x, y, \epsilon) \in \mathbb{A}^3_{xy\epsilon}(R)$ , the action of  $\lambda$  is given by

$$(2.5) \quad \lambda \cdot (x, y, \epsilon) = (\lambda x, \lambda y, \lambda^{-3}\epsilon).$$

Because the action preserves (2.4), one can consider the quotient  $\mathbb{G}_m \backslash \tilde{Y}$ , which is just  $Y$ . Indeed,  $x$  and  $y$  are homogeneous coordinates of degree one, defining the embedding  $\mathbb{G}_m \backslash \tilde{Y} \rightarrow \mathbb{P}^1$ . The coordinate  $\epsilon$  of  $Y$  is redundant, but it will be convenient for later purposes.

**2.2. Construction of the family  $f: X \rightarrow Y$ .** We describe  $f: X \rightarrow Y$  in this subsection. We will define  $X$  as a quotient of  $\tilde{X}$ , where  $\tilde{X}$  is an affine subscheme of  $\mathbb{A}^3_{xy\epsilon} \times \mathbb{A}^3_{uvw}$ . The defining equations of  $\tilde{X}$  are

$$(2.6) \quad h(x, y)\epsilon = 1,$$

$$(2.7) \quad \epsilon \cdot w^2 = h(u, v)(yu - xv).$$

Now we let  $\mathbb{G}_m \times \mathbb{G}_m$  act on  $\tilde{X}$  in the following way. If  $R$  is a ring,  $(\lambda, \mu) \in \mathbb{G}_m(R) \times \mathbb{G}_m(R)$ , and  $(x, y, \epsilon, u, v, w) \in \tilde{X}$ , then we define

$$(2.8) \quad (\lambda, \mu) \cdot (x, y, \epsilon, u, v, w) = (\lambda x, \lambda y, \lambda^{-3}\epsilon, \mu u, \mu v, \lambda^2 \mu^2 w).$$

Since (2.6) and (2.7) are preserved by the action (2.8), we may define

$$(2.9) \quad X = \mathbb{G}_m \times \mathbb{G}_m \backslash \tilde{X}.$$

Furthermore, the projection  $\tilde{X} \rightarrow \tilde{Y}$  descends to  $X \rightarrow Y$ , which we denote by  $f$ .

*Remark 2.1.* Geometrically speaking,  $X$  parametrises the double covers of  $\mathbb{P}^1$  branched along the divisor  $Z \cup \{t\}$  of degree four, as  $t$  varies in  $Y$ . However, this does not uniquely characterise  $X$ , since there is more than one such double cover which is not isomorphic to another over  $\mathbb{Q}$ .

*Remark 2.2.* When  $h(x, y) = x(x - y)y$ ,  $Y$  can be identified with the affine line without 0 and 1 by taking  $\lambda = x/y$  as an affine coordinate. Then, the equation

$$(2.10) \quad w^2 = u(u - v)v(u - \lambda v)$$

defines the Legendre family of elliptic curves over  $Y$ . Our family  $X \rightarrow Y$  of elliptic curves in this case is represented by

$$(2.11) \quad (x(x - y)y^2)^{-1}w^2 = u(u - v)v(u - \lambda v),$$

so one can view it as a quadratic twist of the original Legendre family by  $x(x - y)y^2$ . This relation between Legendre family and our  $X$  is available because of the affine coordinate  $\lambda$  for  $Y$ . When  $h(x, y)$  has no rational linear factor, such an affine coordinate is not available, whence the original Legendre family does not directly generalise. It is the advantage of the twisted family (2.11) that it generalises to general  $h(x, y)$ .

**2.3. Properties of  $f: X \rightarrow Y$ .** In this subsection, we study basic properties of  $f: X \rightarrow Y$ . For some ring  $R$  and  $t = (x_t : y_t) \in Y(R)$ , the elliptic curve  $X_t$  is defined by the equation

$$(2.12) \quad X_t : \epsilon \cdot w^2 = h(u, v)(y_t u - x_t v),$$

which may be interpreted as a quadratic twist of

$$(2.13) \quad X'_t : w^2 = h(u, v)(y_t u - x_t v)$$

by  $\epsilon$ , although  $X'_t$  does not patch together to form a family of elliptic curves over  $Y$ . In fact,  $X'_t$  is not even well-defined on the projective equivalence class of  $t = (x_t : y_t)$ , and only its quadratic twist  $X_t$  is well-defined. In any case, we can compute the discriminant of the right hand side of (2.13), as well as prove its properties.

**Proposition 2.1.** *The discriminant of the right hand side of (2.13) is*

$$(2.14) \quad h(x_t, y_t)^2 \cdot \delta$$

where  $\delta$  is the discriminant of  $h(x, y)$ . Furthermore, we have:

- (1) if  $t \in Y(\mathbb{Z}_S)$ , then  $X'_t$  has good reduction outside  $S$  and  $2\delta$ ;
- (2) if an odd prime  $p \in S$  is a prime of bad reduction for  $X'_t$  and  $p$  does not divide  $2\delta$ , then  $h(x, y) = 0$  has at least one solution modulo  $p$ ;
- (3) if  $p$  does not divide  $2\delta$ , then  $X'_t$  has either good or multiplicative reduction.

*Proof.* The formula (2.14) follows from the representation of the discriminant in terms of differences of roots. Indeed, if  $P(x)$  is a polynomial of one variable with roots  $\alpha_1, \dots, \alpha_n$ , then the discriminant  $\delta_P$  of  $P(x)$  is

$$(2.15) \quad \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

If  $P(x) = (x - \beta)Q(x)$  and  $\alpha_n = \beta$ , then the above formula can be rewritten

$$(2.16) \quad \prod_{i < n} (\beta - \alpha_i)^2 \times \prod_{i < j < n} (\alpha_i - \alpha_j)^2,$$

which equals  $P_1(\beta)^2 \cdot \delta_Q$ .

If  $t \in Y(\mathbb{Z}_S)$  and  $(x_t : y_t)$  is some representative of  $t$ , then  $X'_t$  has good reduction away from  $S$  and  $2\delta$ . Indeed, a double cover of  $\mathbb{P}^1$  branched along four distinct points is smooth away from characteristic two.

Suppose  $p \in S$  does not divide  $2\delta$  and  $X'_t$  has bad reduction at  $p$ . Since  $p$  does not divide  $\delta$ ,  $h(x, y)$  has three distinct roots modulo  $p$ . Thus  $X'_t$  has bad reduction if and only if  $t$  coincides with one of three zeroes of  $h(x, y)$ . In particular,  $t$  is a solution of  $h(x, y) = 0$  modulo  $p$ .

Assume that  $p$  does not divide  $2\delta$  and  $X'_t$  has bad reduction at  $p$ . Then the right hand side of (2.13) cannot have a cubic factor, since such a factor will force  $h(x, y)$  to have at least a square factor modulo  $p$ , contradicting the assumption. In other words,  $X'_t$  has either good or multiplicative reduction. This completes the proof of the proposition. □

For  $X_t$ , we can prove the following.

**Proposition 2.2.** *With the notation as in the previous proposition, the discriminant of (2.12) is*

$$(2.17) \quad h(x_t, y_t)^4 \delta.$$

*In particular, for any  $t \in Y(\mathbb{Z}_S)$ ,  $X_t$  has good reduction outside  $S$  and  $2\delta$ .*

*Proof.* This follows immediately from Proposition 2.1 and the description of the discriminant in terms of differences of roots. □

*Remark 2.3.* The dependence of  $X'_t$  on the choice of representative  $(x_t : y_t)$  is not so serious, as far as we work with rational numbers. We can always take  $(x_t : y_t)$  such that  $x_t$  and  $y_t$  are relatively prime integers and  $x_t$  is non-negative. If we work over a number field which has either class number larger than 1 or units other than  $\pm 1$ , this is not straightforward. Working with  $X'_t$  has the advantage that the conductor of  $X'_t$  is usually smaller than  $X_t$  and it has in some sense finer information about  $t$  than  $X_t$  does. On the other hand,  $X_t$  is associated in a natural way to  $t$ , and its isomorphism class is independent of the choice of a representative  $(x_t : y_t)$  for  $t$ , so it is technically more convenient.

### 3. DEFINING EQUATIONS FOR THE FIBRES OF $\kappa$

In the previous section, we defined a map

$$(3.1) \quad \kappa : t \mapsto X_t$$

which associates an elliptic curve  $X_t$  to a solution  $t \in Y(\mathbb{Z}_S)$ . The aim of the present section is to describe  $\kappa^{-1}(E)$  as a variety defined by explicit polynomials.

**3.1. Some invariant theory.** We briefly review some basic invariant theory of binary forms that is relevant for us. We start with invariants of binary quartic forms.

Let

$$(3.2) \quad q = A_0u^4 + A_1uv^3 + A_2u^2v^2 + A_3uv^3 + A_4v^4$$

be a generic binary quartic form in  $u, v$ , with coefficients  $A_i$ 's. We choose

$$(3.3) \quad I_2 = \frac{1}{12}A_2^2 - \frac{1}{4}A_1A_3 + A_0A_4,$$

$$(3.4) \quad I_3 = \frac{1}{216}A_2^3 - \frac{1}{48}A_1A_2A_3 + \frac{1}{16}A_0A_3^2 + \frac{1}{16}A_1^2A_4 - \frac{1}{6}A_0A_2A_4$$

as generators for the ring of invariants of binary quartic forms. Note that they have rational coefficients, and their degrees are two and three respectively.

In fact, these two invariants are algebraically independent; in other words, the ring of invariants is isomorphic to the polynomial ring in two variables. To stress the dependence of the invariants on the coefficients, we denote by  $q(A)$  the quartic form with coefficients  $A = (A_0, A_1, A_2, A_3, A_4)$  and denote their invariants by  $I_2(A)$  and  $I_3(A)$  respectively.

**Proposition 3.1.** *Let  $q(A)$  and  $q(A')$  be two binary quartic forms with rational coefficients. They are linearly equivalent over  $\mathbb{Q}$  if and only if there exists  $\lambda \in \mathbb{Q}^\times$  such that*

$$(3.5) \quad I_2(A) = \lambda^2(A'),$$

$$(3.6) \quad I_3(A) = \lambda^3(A')$$

hold.

*Proof.* Classical invariant theory. □

Now we consider the invariant theory of a pair of binary forms. Let

$$(3.7) \quad q(A, B) = (A_0u + A_1v)(B_0u^3 + B_1u^2v + B_2uv^2 + B_3v^3)$$

be a product of a binary linear form and a binary cubic form, where  $A = (A_0, A_1)$  and  $B = (B_0, \dots, B_3)$  denote the coefficients of a linear form and a cubic form respectively. Two invariants

$$(3.8) \quad c_4(A, B) = -16(-A_1^2B_1^2 + 3A_1^2B_0B_2 + A_0A_1B_1B_2 - A_0^2B_2^2 - 9A_0A_1B_0B_3 + 3A_0^2B_1B_3),$$

$$(3.9) \quad c_6(A, B) = -32(2A_1^3B_1^3 - 9A_1^3B_0B_1B_2 - 3A_0A_1^2B_1^2B_2 + 18A_0A_1^2B_0B_2^2 - 3A_0^2A_1B_1B_2^2 + 2A_0^3B_2^3 + 27A_1^3B_0^2B_3 - 27A_0A_1^2B_0B_1B_3 + 18A_0^2A_1B_1^2B_3 - 27A_0^2A_1B_0B_2B_3 - 9A_0^3B_1B_2B_3 + 27A_0^3B_0B_3^2)$$

generate the ring of invariants.

We digress for a discussion on the relation between the above invariants and invariants of an elliptic curve often used in the literature. If an elliptic curve  $E$  is given by

$$(3.10) \quad E : y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

then

$$(3.11) \quad c_4(E) = 16a_2^2 - 48a_4,$$

$$(3.12) \quad c_6(E) = -64a_2^3 + 288a_2a_4 - 864a_6$$

are often called the  $c_4$ -invariant and  $c_6$ -invariant of  $E$ . If we take  $A_0 = 0, A_1 = 1, B_0 = 1, B_1 = a_2, B_2 = a_4,$  and  $B_3 = a_6,$  then  $c_4(A, B)$  and  $c_6(A, B)$  are precisely the  $c_4$ -invariant and  $c_6$ -invariant of the elliptic curve defined by (3.10). The discriminant of (3.10) is given by

$$(3.13) \quad \delta(E) = -16(-a_2^2a_4^2 + 4a_2^3a_6 + 4a_4^3 - 18a_2a_4a_6 + 27a_6^2),$$

and it can be alternatively written as

$$(3.14) \quad \delta(E) = 2^63^3(c_4(E)^3 - c_6(E)^2) = 1728(c_4(E)^3 - c_6(E)^2).$$

The discriminant of  $q(A, B)$  is, viewed as a single binary quartic form, equal to

$$(3.15) \quad \delta(q(A, B)) = -(-B_1^2B_2^2 + 4B_0B_2^3 + 4B_1^3B_3 - 18B_0B_1B_2B_3 + 27B_0^2B_3^2) \times (-A_1^3B_0 + A_0A_1^2B_1 - A_0^2A_1B_2 + A_0^3B_3)^2.$$

If we take  $A_0 = 0, A_1 = 1, B_0 = 1, B_1 = a_2, B_2 = a_4,$  and  $B_4 = a_6,$  then two discriminants are related by

$$(3.16) \quad 16 \cdot \delta(q(A, B)) = \delta(E).$$

The relation between  $c_4, c_6$  and the previously introduced  $I_2$  and  $I_3$  is more straightforward. Indeed, they are related by

$$(3.17) \quad \begin{aligned} c_4(q(A, B)) &= 192 \cdot I_2(q(A, B)) \\ &= 2^6 3 \cdot I_2(q(A, B)), \end{aligned}$$

$$(3.18) \quad \begin{aligned} c_6(q(A, B)) &= -13824 \cdot I_3(q(A, B)) \\ &= -2^9 3^3 \cdot I_3(q(A, B)), \end{aligned}$$

where we view  $q(A, B)$  as a product of two forms on the left hand side, while on the right hand side we view it as a single quartic form whose coefficients are quadratic forms in  $A_i$ 's and  $B_i$ 's.

Now we return to the invariant theory of  $q(A, B)$ .

**Proposition 3.2.** *Let  $q(A, B)$  and  $q(A', B')$  be two binary quartic forms with factorisation as a product of a linear and a cubic factor, and suppose that the coefficients  $A, A', B$  and  $B'$  are rational numbers. They are linearly equivalent over the rational numbers if and only if there exists  $\lambda \in \mathbb{Q}^\times$  such that*

$$(3.19) \quad c_4(q(A, B)) = \lambda^4 c_4(q(A', B')),$$

$$(3.20) \quad c_6(q(A, B)) = \lambda^6 c_6(q(A', B'))$$

hold.

*Proof.* Classical invariant theory. □

**3.2. Faithfulness of descent.** The overall strategy is to study  $t \in Y(\mathbb{Z}_S)$  in terms of  $X_t$ . In other words, we consider the map

$$(3.21) \quad \kappa: t \mapsto X_t$$

and try to use  $\kappa$  in order to compute  $Y(\mathbb{Z}_S)$ . To realise this, we will show two key properties of  $\kappa$ :

- (1)  $\kappa$  is an  $n$ -to-1 map, where  $n$  is an explicit integer less than six.
- (2) Given a Weierstrass equation of an elliptic curve  $E$ , one can compute  $\kappa^{-1}(E)$ .

Let us consider the first property of  $\kappa$ . Let  $E$  be an elliptic curve. We would like to count the number of  $t \in Y(\mathbb{Z}_S)$  for which  $X_t$  is isomorphic to  $E$ , where  $E$  is given as a Weierstrass equation

$$(3.22) \quad E: y^2 + a_1y + a_3 = x^3 + a_2x^2 + a_4x + a_6$$

with rational coefficients. On the other hand,  $X_t$  is defined by

$$(3.23) \quad \epsilon w^2 = h(u, v)(yu - xv)$$

where  $h(x, y)\epsilon = 1$ . We rewrite  $X_t$  as

$$(3.24) \quad w^2 = h(u, v)(yu - xv)h(x, y)$$

and let

$$(3.25) \quad Q(x, y, h) = (yu - xv) \cdot h(u, v)h(x, y)$$

be the associated joint quartic form in  $u$  and  $v$ . In fact, one could write  $Q(x, y, h) = Q(t, h)$ , in the sense that  $Q(\lambda x, \lambda y, h)$  is rationally equivalent to  $Q(x, y, h)$  for any  $\lambda \in \mathbb{Q}^\times$ . For simplicity of notation, let

$$(3.26) \quad c_4(x, y, h) = c_4(Q(x, y, h)),$$

$$(3.27) \quad c_6(x, y, h) = c_6(Q(x, y, h))$$

be the invariants of  $Q(x, y, h)$ . The set of all  $t \in Y(\mathbb{Z}_S)$  for which  $X_t$  is isomorphic to  $E$  is defined by the equations

$$(3.28) \quad c_4(x, y, h) = \lambda^4 c_4(E),$$

$$(3.29) \quad c_6(x, y, h) = \lambda^6 c_6(E),$$

where  $c_4(x, y, h)$  and  $c_6(x, y, h)$  are homogeneous polynomials of degree eight and twelve in  $x, y$ , respectively. In fact, we can eliminate  $\lambda$  from the above two equations to obtain

$$(3.30) \quad J_{24}(x, y, h, E) := \lambda^{12} (c_6(E)^2 c_4(x, y, h)^3 - c_4(E)^3 c_6(x, y, h)^2),$$

which factors as

$$(3.31) \quad J_{24}(x, y, h, E) = \lambda^{12} \cdot h(x, y)^6 \cdot J_6(x, y, h, E),$$

where  $J_6(x, y, h, E)$  is the homogeneous polynomial of degree six in variables  $x$  and  $y$ , characterised by the above equality.

**Proposition 3.3.** *The set of points  $t \in Y(\mathbb{Z}_S)$  for which  $X_t$  is isomorphic to  $E$  is in bijection with the projective equivalence classes of solutions of  $J_6(x, y, h, E) = 0$  such that (3.28) and (3.29) have a common solution in  $\lambda$ . In particular, this set has cardinality at most six.*

*Proof.* We first show that  $J_6(x, y, h, E)$ , viewed as a homogeneous polynomial in  $x$  and  $y$ , is not identically zero for an elliptic curve  $E$  and a non-degenerate binary cubic form  $h(x, y)$ . We work with complex numbers, although any algebraically closed field of characteristic zero suffices for our purpose. Let  $(x_i, y_i)$  with  $i = 1, 2, \dots, r$  be a sequence of non-equivalent complex zeros of  $J_6(x, y, h, E)$ . They are precisely the values for which

$$(3.32) \quad Q_i(x_i, y_i, h) = (y_i u - x_i v) \cdot h(u, v) h(x_i, y_i)$$

becomes equivalent to

$$(3.33) \quad Q_E := v(u^3 + a_4(E)uv^2 + a_6(E)v^3)$$

as joint binary quartic forms in  $u$  and  $v$ . Here, two joint forms  $Q_i$  and  $Q_E$  are called equivalent if there exists a linear change of variables over complex numbers which transforms  $y_i u - x_i v$  into  $v$  up to multiplication by a non-zero scalar and transforms  $h(u, v)$  into  $u^3 + a_4(E)uv^2 + a_6(E)v^3$  up to multiplication by a non-zero scalar. If we look at how the linear change of variables acts on the points of a projective line with the homogeneous coordinates  $u$  and  $v$ , then such an equivalence sends  $(x_i : y_i)$  to  $(1 : 0)$  and the zeros of  $h(u, v)$  to those of  $u^3 + a_4(E)uv^2 + a_6(E)v^3$ . Since  $E$  is an elliptic curve,  $u^3 + a_4(E)uv^2 + a_6(E)v^3$  has three distinct zeros. Thus there are six projective automorphisms of the projective line which send the zeros of  $h(u, v)$  to those of  $u^3 + a_4(E)uv^2 + a_6(E)v^3$ . Thus  $r$  is at most six, and  $J_6(x, y, h, E)$  cannot be identically zero.

If  $t = (x : y) \in Y(\mathbb{Z}_S)$ , then  $h(x, y) \neq 0$ . By (3.31), the vanishing of  $J_{24}(x, y, h, E)$  is equivalent to that of  $J_6(x, y, h, E)$ . If, further,  $t$  is such that  $X_t$  is isomorphic to  $E$ , then clearly (3.28) and (3.29) have a common solution. Conversely,  $J_6(x, y, h, E)$  vanishes for each solution  $t = (x : y)$  of (3.28) and (3.29). Thus such  $t$  together with  $\lambda$  gives rise to  $X_t$  equipped with an isomorphism to  $E$ . This completes the proof.  $\square$

**Corollary 3.1.** *For a fixed elliptic curve  $E$ , the number of  $t \in Y(\mathbb{Z}_S)$  for which  $X_t$  is isomorphic to  $E$  is at most the cardinality of  $\text{Aut}_{\mathbb{Q}}(Y)$ .*

*Proof.* This is implicit in the proof of Proposition 3.3, observing that the isomorphisms between  $h(u, v)$  and  $u^3 + a_4(E)uv^2 + a_6(E)v^3$  form a torsor for  $\text{Aut}_{\mathbb{Q}}(Y)$ .  $\square$

Before we move on, we analyse the coefficients of  $J_6(x, y, h, E)$ . As we mentioned earlier, it is homogeneous of degree six in  $x$  and  $y$ . With respect to the coefficients of  $h(x, y)$ , namely  $a, b, c$ , and  $d$ , it is homogeneous of degree six as well. In terms of coefficients of  $E$ , it has degree twelve in the following sense. If we write  $E$  as

$$(3.34) \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then  $J_6(x, y, h, E)$  is a polynomial in variables  $a_1, a_2, a_3, a_4$  and  $a_6$ . If we take the degree of  $a_m$  to be  $m$ , then  $J_6(x, y, h, E)$  is homogeneous of degree twelve in  $a_1, \dots, a_6$ . More concretely, if we take a model of  $E$  for which  $a_1 = a_2 = a_3 = 0$ , then each term of  $J_6(x, y, h, E)$ , viewed as a polynomial in  $a_4$  and  $a_6$ , is either  $a_4^3$  or  $a_6^2$ . Based on this observation, we arrange

$$(3.35) \quad J_6(x, y, h, E) = \sum_{i=0}^6 (C_i^*(h)a_4^3 + D_i^*(h)a_6^2) x^{6-i} y^i$$

where  $C_i^*(h)$  and  $D_i^*(h)$  are homogeneous polynomials of degree six in  $a, b, c$ , and  $d$ . In fact, all of them have a large integer factor, so we let

$$(3.36) \quad C_i^*(h) = 2^{22}3^3 C_i(h) \text{ and } D_i^*(h) = 2^{22}3^3 D_i(h)$$

and give formulas for  $C_i(h)$  and  $D_i(h)$ :

$$\begin{aligned} C_0(h) &= (2c^3 - 9bcd + 27ad^2)^2, \\ D_0(h) &= -27(-c^2 + 3bd)^3, \\ C_1(h) &= -6(2c^3 - 9bcd + 27ad^2)(-bc^2 + 6b^2d - 9acd), \\ D_1(h) &= -81(-bc + 9ad)(-c^2 + 3bd)^2, \\ C_2(h) &= -3(b^2c^4 - 24ac^5 + 18b^3c^2d + 90abc^3d - 108b^4d^2 \\ &\quad + 216ab^2cd^2 - 567a^2c^2d^2 + 486a^2bd^3), \\ D_2(h) &= -81(-c^2 + 3bd)(2b^2c^2 - 3ac^3 - 3b^3d - 9abcd + 81a^2d^2), \\ C_3(h) &= -2(13b^3c^3 - 72abc^4 - 72b^4cd + 567ab^2c^2d \\ &\quad - 432a^2c^3d - 432ab^3d^2 + 243a^2bcd^2 + 729a^3d^3), \\ D_3(h) &= -27(-bc + 9ad)(7b^2c^2 - 18ac^3 - 18b^3d + 36abcd + 81a^2d^2), \end{aligned}$$

$$\begin{aligned}
 C_4(h) &= -3(b^4c^2 + 18ab^2c^3 - 108a^2c^4 - 24b^5d + 90ab^3cd \\
 &\quad + 216a^2bc^2d - 567a^2b^2d^2 + 486a^3cd^2), \\
 D_4(h) &= -81(-b^2 + 3ac)(2b^2c^2 - 3ac^3 - 3b^3d - 9abcd + 81a^2d^2), \\
 C_5(h) &= 6(b^2c - 6ac^2 + 9abd)(2b^3 - 9abc + 27a^2d), \\
 D_5(h) &= -81(-bc + 9ad)(-b^2 + 3ac)^2, \\
 C_6(h) &= (2b^3 - 9abc + 27a^2d)^2, \\
 D_6(h) &= -27(-b^2 + 3ac)^3.
 \end{aligned}$$

The above coefficients seem to have certain invariant theoretic meanings, but for the purpose of the current article, we only need to regard  $J_6(x, y, h, E)$  as a defining equation of  $\kappa^{-1}(E)$  given as explicitly as possible.

#### 4. MAIN THEOREMS

Now we are ready to state and prove our main theorems. Before we state our result, recall that the strategy was to consider

$$(4.1) \quad \kappa: t \mapsto X_t$$

and study  $t$  in terms of  $X_t$ . In the previous subsection, we focused on the analysis of  $\kappa^{-1}(E)$  for a fixed  $E$ . What remains is to consider the image of  $\kappa$ .

Among several approaches to analyse the image of  $\kappa$ , the common fundamental property of  $\kappa$  is that  $X_t$  has good reduction outside  $2\delta$  and  $S$ . It is convenient to introduce notation for the number of such curves.

**Definition 4.1.** Let  $N$  be a positive integer. Let  $g(N)$  be the number of isomorphism classes of elliptic curves whose conductor is  $N$ . For a finite set  $S$  of primes, let

$$(4.2) \quad M = \prod_{p \in S} p$$

and let  $G(S)$  be the number of isomorphism classes of elliptic curves which have good reduction outside  $S$ .

**Theorem 4.1.** *Let  $\varepsilon$  be any positive real. Then there exist positive numbers  $k_1, k_2$  depending only on  $\varepsilon$ , such that*

$$(4.3) \quad g(N) < k_1 N^{\frac{1}{2} + \varepsilon},$$

$$(4.4) \quad G(S) < k_2 M^{\frac{1}{2} + \varepsilon}$$

*hold. If we assume (a part of) the BSD conjecture and the generalised Riemann hypothesis for the elliptic curves  $y^2 = x^3 + n$ ,  $n \in \mathbb{Z}$ , then there exist constants  $k_4$  and  $k_5$  for which*

$$(4.5) \quad G(S) < k_4 M^{\frac{k_5}{\log \log M}}$$

*holds.*

*Proof.* See Brumer and Silverman [4], Theorem 1 and Theorem 4. □

As a corollary of the above theorem, we obtain a first, rather crude, upper bound for the cardinality of  $Y(\mathbb{Z}_S)$ .

**Theorem 4.2.** *Assume that  $S$  contains 2 and prime divisors of  $\delta$ . Then*

$$(4.6) \quad |Y(\mathbb{Z}_S)| < |\text{Aut}_{\mathbb{Q}}(Y)| \times G(S).$$

*In particular, we have for every real  $\varepsilon > 0$ ,*

$$(4.7) \quad |Y(\mathbb{Z}_S)| < |\text{Aut}_{\mathbb{Q}}(Y)| \times k_2 M^{\frac{1}{2} + \varepsilon}$$

*where  $M$  is the product of all prime numbers in  $S$ , and  $k_2$  is the number from Theorem 4.1. Under the assumption of the generalised Riemann hypothesis and the BSD conjecture for the curve  $y^2 = x^3 + n$ , we have*

$$(4.8) \quad |Y(\mathbb{Z}_S)| < |\text{Aut}_{\mathbb{Q}}(Y)| \times k_4 M^{\frac{k_5}{\log \log M}},$$

*where  $k_4$  and  $k_5$  are absolute constants.*

*Proof.* The first assertion follows from Proposition 3.3 and Corollary 3.1. The second follows from the first assertion combined with Theorem 4.1. □

*Remark 4.1.* In the course of deriving the above upper bound, we have forgotten all information of  $X_t$  except the divisors of the conductors of  $X_t$ . Numerical computations indicate that the reduction types at the primes dividing  $2\delta$  take a particular form, which will facilitate practical computations.

**4.1. Comparison with Evertse’s bound.** Evertse proved the following remarkable upper bound.

**Theorem 4.3.** *Let  $h(x, y)$  be an integral binary form of degree  $n \geq 3$  which is divisible by at least three pairwise linearly independent linear forms in some algebraic number field. Let  $p_1, p_2, \dots, p_s$  be a sequence of distinct primes. The equation*

$$(4.9) \quad |h(x, y)| = \prod_{i=1}^s p_i^{e_i}$$

*in relatively prime integers  $x, y$  and non-negative integers  $e_1, e_2, \dots, e_s$  has at most*

$$(4.10) \quad 2 \times 7^{n^3(2s+3)}$$

*solutions. There is an analogous explicit upper bound for number fields.*

*Proof.* See Corollary 2 of [10]. □

We note that under the additional assumption that  $h(x, y)$  is irreducible, Evertse [11] obtained an upper bound  $(5 \cdot 10^6 \cdot n)^s$  which is significantly better than (4.10) as  $n$  grows. Since we are only treating the case  $n = 3$ , both upper bounds have the same asymptotic growth in  $s$ .

As a direct consequence of Theorem 4.3, we obtain

$$(4.11) \quad |Y(\mathbb{Z}_S)| < 7^{54s+81}$$

when  $s$  is the cardinality of  $S$ . Let us take  $S$  to be the set

$$(4.12) \quad S = \{p : p < T\}$$

of all primes up to a positive number  $T$ . Then by the prime number theorem  $s$  is asymptotically  $T/\log T$ . Therefore, Evertse's bound can be rewritten, in a logarithmic scale, as

$$(4.13) \quad \log |Y(\mathbb{Z}_S)| = O\left(\frac{T}{\log T}\right).$$

On the other hand, the standard estimate shows that

$$(4.14) \quad \log M = \sum_{p < T} \log p = O(T)$$

and our unconditional upper bound of Theorem 4.1 becomes

$$(4.15) \quad \log |Y(\mathbb{Z}_S)| = O(T).$$

The conditional upper bound of Theorem 4.1 becomes

$$(4.16) \quad \log |Y(\mathbb{Z}_S)| = O\left(\frac{\log M}{\log \log M}\right) = O\left(\frac{T}{\log T}\right),$$

which is comparable to Evertse's.

Putting aside the comparisons between the upper bounds for the cardinalities  $Y(\mathbb{Z}_S)$ , we point out the crucial difference between our method and Evertse's in terms of effectiveness. Evertse's upper bound is ineffective, in the sense that it does not provide an algorithm to decide  $Y(\mathbb{Z}_S)$ . In contrast, our proof is manifestly constructive, especially if one combines it with modularity of elliptic curves. We elaborate on the constructive aspects of our method in the next section.

## 5. ALGORITHMIC ASPECTS

In this subsection, we elaborate on the algorithmic aspects of our proof. Effectiveness of a proof of the finiteness of  $Y(\mathbb{Z}_S)$  can be formulated in at least two ways:

- (1) to have an explicit upper bound on the height of  $t \in Y(\mathbb{Z}_S)$  in terms of the coefficients of  $h(x, y)$  and  $S$ ,
- (2) to have a procedure which enables one to determine  $Y(\mathbb{Z}_S)$ , in a provably finite amount of time, for a numerically given  $h(x, y)$  and  $S$ .

The first version of effectiveness implies the second. Indeed, if  $T$  is such a bound, then factoring  $h(m, n)$  as  $m$  and  $n$  vary among all integers with absolute value at most  $T$ , one can determine  $Y(\mathbb{Z}_S)$ . In fact, Baker's method in principle provides such an upper bound. However, the efficiency of such a procedure depends on the size of  $T$ , and the astronomical size of the numbers obtained from Baker's bound often prevents one from computing  $Y(\mathbb{Z}_S)$  in practice. Our method directly provides the second version of effectiveness without an a priori upper bound for height of  $t \in Y(\mathbb{Z}_S)$ , and we shall describe the procedure as it is implemented in a computer algebra package in order to generate tables of numerical examples.

Recall that the principal tool for us is the map

$$(5.1) \quad \kappa: t \mapsto X_t$$

which associates an elliptic curve  $X_t$  to a putative solution  $t$ . Computation of  $\kappa^{-1}(E)$  amounts to solving polynomials in one variable, such as  $J_6(x, y, h, E)$ . In particular,  $\kappa^{-1}(E)$  can be effectively decided once the coefficients of  $E$  are known.

Thus, what remains is to determine all possible elliptic curves  $E$  for which  $\kappa^{-1}(E)$  is possibly non-empty.

**Theorem 5.1.** *For a finite set  $S$  of prime numbers, the coefficients of isomorphism classes of elliptic curves which have good reduction outside  $S$  can be determined algorithmically.*

*Proof.* We give a brief description. For details, especially practical issues, we refer to Cremona. Using the modularity theorem, one may compute the isogeny classes of elliptic curves by means of modular forms. The space of modular forms can be computed using modular symbols for example. For each isogeny class of elliptic curves, one can decide the isomorphism classes of elliptic curves contained in it. In fact, there are at most eight isomorphism classes in a fixed isogeny class, by a theorem of Kenku [12].  $\square$

This modular approach allows us, as a by-product, to obtain a new bound for the cardinality of  $Y(\mathbb{Z}_S)$ .

**Theorem 5.2.** *Let  $S$  contain all prime divisors of  $2\delta$ . Let*

$$(5.2) \quad M_1 = \prod_{p \in S} p^{2+d_p}$$

where  $d_2 = 6$ ,  $d_3 = 3$ , and  $d_p = 0$  for  $p \geq 5$ . Let  $X_0(M_1)$  be the modular curve of level  $\Gamma_0(M_1)$ , and let  $g_0(M_1)$  be its genus. Then,

$$(5.3) \quad |Y(\mathbb{Z}_S)| < 8 \times |\text{Aut}_{\mathbb{Q}}(Y)| \times g_0(M_1).$$

Note that  $g_0(M_1) < M_1$ .

*Proof.* The dimension of space of cusp forms of weight two on  $X_0(M_1)$  is equal to the genus of  $X_0(M_1)$ . For each rational Hecke eigenform of weight two, there are at most eight isomorphism classes of elliptic curves by Kenku's theorem. For each elliptic curve, there are at most  $|\text{Aut}_{\mathbb{Q}}(Y)|$  elements of  $Y(\mathbb{Z}_S)$ . Thus we obtain the claimed bound.  $\square$

*Remark 5.1.* The above bound is clearly worse than previous ones, as  $g_0(M_1)$  is roughly  $M_1$ . Nevertheless, the proof of the above bound uses the modularity theorem as its key ingredient, and it has little to do with estimation of number of points on the curve  $y^2 = x^3 + n$ .

In order to compute  $Y(\mathbb{Z}_S)$  in practice, one has to first tabulate the elliptic curves. By a tabulation of elliptic curves, we shall mean the table of isomorphism classes of elliptic curves, represented in a Weierstrass equation, ordered by their conductors. In a sense this step of tabulation is a pre-computation, which only depends on the discriminant of  $h(x, y)$ , and the table can be used again and again.

## 6. NUMERICAL EXAMPLES

We give numerical examples in this section. As explained before, the crucial step in working out a numerical example is to tabulate elliptic curves with a specified conductor. We avoid this step by relying on Cremona's Elliptic Curve Database. In particular, we assume the following throughout.

**Hypothesis.** *Cremona's Elliptic Curve Database is complete (i.e., no curve is omitted) up to conductor 350,000.*

We will compute  $Y(\mathbb{Z}_S)$  based on Cremona’s database. The completeness of the list of the solutions depends on the truth of the hypothesis. More specifically, we need a complete list of elliptic curves which has good reduction outside  $2\delta$  and  $S$ .

We give some justification for introducing the above hypothesis. If some elliptic curves with conductor less than 350,000 turn out to be omitted in Cremona’s table, then it is possible that these new elliptic curves give rise to new solutions, which are not listed in the present paper. Such corrections can always be made upon each discovery, if any, of omitted elliptic curves. On the other hand, it is clearly beyond the scope of the current work to check that the computer codes which were used to generate Cremona’s table contain no bugs.

**6.1. Implementation and performance.** In this subsection, we explain how we implement the algorithm into a computer algebra package and its performance. What we do *not* compute is the necessary table of elliptic curves. We assume that a list of elliptic curves of a specified conductor is already available.

In order to faithfully follow the proof of finiteness of  $Y(\mathbb{Z}_S)$ , we should compute a set of elliptic curves which contains  $\kappa(Y(\mathbb{Z}_S))$  and compute  $\kappa^{-1}(E)$  for each curve  $E$  in the set. For example, one might choose to compute the set of elliptic curves whose conductor divides  $M_1$  of (5.2). However, this is computationally inefficient for the following reason. When we replace  $E$  by its quadratic twist,  $J_6(x, y, h, E)$  is replaced by its multiple. It follows that one has to solve the same polynomial  $2^{s+1}$  times when  $s$  is the cardinality of  $S$ . It turns out that working with  $X'_t$  we avoid this problem of solving  $J_6(x, y, h, E)$  repeatedly.

The following proposition tells us why it is possible to compute  $Y(\mathbb{Z}_S)$  using  $X'_t$  instead of  $X_t$ .

**Proposition 6.1.** *Let  $E$  be an elliptic curve. There exists  $t \in Y(\mathbb{Z}_S)$  such that  $X_t$  is isomorphic to a quadratic twist of  $E$  if and only if  $J_6(x, y, h, E)$  has a rational solution.*

*Proof.* Recall that we proved that  $J_6(x, y, h, E)$ , (3.28), and (3.29) have a common solution if and only if  $E$  is isomorphic to  $X_t$  itself, without a quadratic twist. Hence, the “only if” part is obvious, and we are left to prove the “if” part of the proposition. It suffices to show that given a solution of  $J_6(x, y, h, E)$ , one can find a quadratic twist  $E'$  of  $E$  such that  $J_6(x, y, h, E')$ , (3.28), and (3.29) have a common solution.

In order to see that finding such a quadratic twist  $E'$  is possible, recall that  $J_{24}(x, y, h, E)$  was defined by

$$(6.1) \quad J_{24}(x, y, h, E) := \lambda^{12} (c_6(E)^2 c_4(x, y, h)^3 - c_4(E)^3 c_6(x, y, h)^2).$$

Let  $E$  be given by the equation

$$(6.2) \quad E: y^2 = x^3 + a_4x + a_6$$

and let  $E'$  be the quadratic twist

$$(6.3) \quad E': y^2 = x^3 + a_4r^2x + a_6r^3$$

of  $E$  by  $r$ . Then the formula for  $J_{24}(x, y, h, E)$ , together with the relations (3.11) and (3.12), tells us that

$$(6.4) \quad J_{24}(x, y, h, E') = r^6 \cdot J_{24}(x, y, h, E).$$

In particular, from factorisation (3.31), it follows that

$$(6.5) \quad J_6(x, y, h, E') = r^6 \cdot J_6(x, y, h, E).$$

So what remains is to find a value of  $r$ , for a given zero  $(x_0, y_0)$  of  $J_6(x, y, h, E')$  (or  $J_6(x, y, h, E)$ ), for which

$$(6.6) \quad c_4(x_0, y_0, h) = \lambda^4 c_4(E'),$$

$$(6.7) \quad c_6(x_0, y_0, h) = \lambda^6 c_6(E')$$

have a rational solution in  $\lambda$ . The above equations are nothing but the equations (3.28) and (3.29) written for  $E'$ . Solving for  $\lambda$ , we get

$$(6.8) \quad \begin{aligned} \lambda^2 &= \frac{c_6(x_0, y_0, h)}{c_4(x_0, y_0, h)} \times \frac{c_4(E')}{c_6(E')} \\ &= \frac{c_6(x_0, y_0, h)}{c_4(x_0, y_0, h)} \times \frac{c_4(E)}{c_6(E)} \times r^{-1}, \end{aligned}$$

so one can take

$$(6.9) \quad r = \frac{c_6(x_0, y_0, h)}{c_4(x_0, y_0, h)} \times \frac{c_4(E)}{c_6(E)}$$

in order to render (6.6) and (6.7) to have solution  $\lambda = \pm 1$ . The assertion of the proposition is proved. □

Based on Proposition 6.1, we proceed as follows in order to compute  $Y(\mathbb{Z}_S)$ . Suppose we are given  $h(x, y)$  and  $S$ . From this, one can compute the list of conductors of  $X'_t$  for  $t \in Y(\mathbb{Z}_S)$ , with negligible computational cost. Using Cremona's Elliptic Curve Database, we get a sequence of elliptic curves  $E_1, E_2, \dots, E_k$ , for some finite  $k$ , where each  $E_i$  is given in a Weierstrass form. Now we compute rational solutions of  $J_6(x, y, h, E_i)$  for each  $E_i$ . If there is a solution, say  $x_t$  and  $y_t$ , then we proceed to compute  $h(x_t, y_t)$  and double check that the result is correct.

As we observed before, the coefficients of  $J_6(x, y, h, E)$  have a large common factor when we start from an elliptic curve with  $a_1 = a_2 = a_3 = 0$ . More precisely, we may take

$$(6.10) \quad J'_6(x, y, h, E) = 2^{-22} \cdot 3^{-3} \cdot J_6(x, y, h, E)$$

whose coefficients are still integral.

We give three examples of  $h$  and present corresponding  $J'_6(x, y, h, E)$  for a generic elliptic curve

$$(6.11) \quad E: y^2 = x^3 + a_4x + a_6.$$

Take

$$(6.12) \quad h_1(x, y) = x^2y - xy^2 = x(x - y)y,$$

which corresponds to the unit equation. In this case,

$$(6.13) \quad J'_6(x, y, h_1, E) = (x - 2y)^2(x + y)^2(2x - y)^2a_4^3 + 27(x^2 - xy + y^2)^3a_6^2,$$

which has a particularly nice factorisation. In this case, the solutions  $(2, 1)$ ,  $(1, -1)$ , and  $(1, 2)$  for  $h_1(x, y) = \pm 2^a$  are clearly visible from the factors of coefficients of  $a_4$ , corresponding to curves with  $a_6 = 0$ . As a less trivial example, we take

$$(6.14) \quad E_{960e6}: x^3 - x^2 - 21345x - 1190943,$$

which is the minimal Weierstrass equation for elliptic curve “960e6” in Cremona’s database. We make a change of variables  $x \mapsto x + 1/3$ ,

$$(6.15) \quad E: y^2 = x^3 - \frac{64036}{3}x - \frac{32347568}{27},$$

for which

$$(6.16) \quad \begin{aligned} & J'_6(x, y, h_1, E) \\ &= -64(3x - 128y)(3x + 125y)(125x - 128y)(125x + 3y)(128x - 125y)(128x - 3y), \end{aligned}$$

and indeed  $(3, 128)$  belongs to  $Y(\mathbb{Z}_S)$  for  $S = \{2, 3, 5\}$ , because  $128 = 2^7$ , and  $128 - 3 = 125 = 5^3$ . The other five factors correspond to orbits of  $\text{Aut}_{\mathbb{Q}}(Y)$ .

As an example for which  $\kappa^{-1}(E)$  has no rational point, we take

$$(6.17) \quad E_{960e5}: y^2 = x^3 - x^2 - 18465x + 971937,$$

which is the curve “960e5”, which is just next to the previous one. After a routine change of variables  $x \mapsto x + 1/3$ , we obtain

$$(6.18) \quad \begin{aligned} J'_6(x, y, h_1, E) &= -64(25x^2 - 13874xy + 25y^2)(25x^2 + 13824xy - 13824y^2) \\ &\quad \times (13824x^2 - 13824xy - 25y^2), \end{aligned}$$

which is a product of three irreducible quadratic polynomials. It follows that there is no solution  $t \in Y(\mathbb{Z}_S)$  with  $S = \{2, 3, 5\}$  for which  $X'_t$  is isomorphic to  $E_{960e5}$ .

Let us consider a different cubic form,

$$(6.19) \quad h_2(x, y) = x^2y + 7y^3 = (x^2 + 7y^2)y,$$

which corresponds to the Ramanujan-Nagell equation. In this case,

$$(6.20) \quad J'_6(x, y, h_2, E) = 2^27^4y^2(9x^2 + 7y^2)^2a_4^3 - 3^37^3(3x^2 - 7y^2)^3a_6^2$$

has again a nice factorisation. Take

$$(6.21) \quad E_{210e1} : y^2 + xy = x^3 + 210x + 900,$$

which is isomorphic to

$$(6.22) \quad y^2 = x^3 + \frac{10079}{48}x + \frac{762481}{864}$$

for which

$$(6.23) \quad J'_6(x, y, h_2, E) = \frac{7}{1024}(45x - 47y)(45x + 47y)(2048x^2 - 14805xy + 113561y^2) \\ \times (2048x^2 + 14805xy + 113561y^2).$$

The solution (47, 45) corresponds to

$$(6.24) \quad h_2(47, 45) = 737280 \\ = 2^{14} \cdot 3^2 \cdot 5,$$

which is an element of  $Y(\mathbb{Z}_S)$  for  $S = \{2, 3, 5\}$ .

Finally, take

$$(6.25) \quad h_3(x, y) = x^3 - x^2y - 4xy^2 - y^3$$

whose discriminant is  $13^2$ . In this case,

$$(6.26) \quad J'_6(x, y, h_3, E) = 13^2(5x^3 + 21x^2y + 6xy^2 - 5y^3)^2a_4^3 + 3^313^3(x^2 + xy + y^2)^3a_6^2,$$

which shows that the coefficients of  $a_4^3$  in general have irreducible factor of degree three. Of course, the squares and cubes in the coefficients are expected, as we have defined  $J_6(x, y, h, E)$  by (3.30) and (3.31).

In practice, the coefficients  $a_4$  and  $a_6$  are very large, so it is difficult to factor  $J'_6(x, y, h, E)$  manually. Nonetheless, using suitable computer algebra packages, one can factor such polynomials rather quickly. The author's experience shows that SageMathCloud is able to factor roughly 200 polynomials per second.

Take  $h(x, y) = h_1(x, y)$  as above, and take  $S = \{2, 7, 11, 13\}$ . Then we need a table of elliptic curves whose conductor divides  $2^8 \cdot 7 \cdot 11 \cdot 13 = 256256$ . Since  $256256 < 350000$  we may use Cremona's Elliptic Curve Database, from which we get 940 such curves. From them, we get 51 solutions, as we display in Table 8.1. It took 4.13 seconds in CPU time to generate Table 8.1. A typical box in the table looks like

$$(6.27) \quad \begin{array}{c} (x_t, y_t) \\ h(x_t, y_t) \\ \text{Factorisation of } h(x_t, y_t) \\ \text{Cremona's label} \\ \text{Factorisation of the conductor} \end{array}$$

with five items listed vertically.

Let us take  $S = \{2, 3, 5, 7\}$  for  $h_2(x, y)$ . In this case, we need elliptic curves of the conductor dividing  $2^8 \cdot 3 \cdot 5 \cdot 7^2 = 188160$ , which is smaller than 350000. Cremona's table contains 4568 such curves, from which we find 33 solutions. It took 20.09 seconds in CPU time to generate Table 8.4.

Let us take  $S = \{2, 5, 13\}$  for  $h_3(x, y)$ . In this case, we need elliptic curves of the conductor dividing  $2^8 \cdot 5 \cdot 13^2 = 216320$ , which is smaller than 350000. Cremona's table contains 976 such curves, from which we find 35 solutions. It took 4.20 seconds in CPU time to generate Table 8.13. Since we wrote a computer code which computes the solutions with  $y_t \neq 0$ , the trivial solution  $h(1, 0) = 1$  is omitted from the table.

*Remark 6.1.* Repeated 6's on the exponent of 2 in the conductors appearing in Table 8.1 can be perhaps predicted by considering connected components in the Neron model. On the other hand, as the 2 divides the discriminant of  $h_2(x, y)$ , various exponents of 2 appear in Table 8.4. Although we ignored further analysis of conductors of  $X'_t$  at the primes dividing  $2\delta$ , such an analysis might help practical computations.

**6.2. Statistics for  $x(x - y)y$ .** In this section, we fix

$$(6.28) \quad h(x, y) = x(x - y)y$$

and vary  $S$  in a few directions. Let us begin with the case when

$$(6.29) \quad S = \{2, p\}$$

consists of 2 and one more prime  $p$ . Cremona's database allows us to compute  $Y(\mathbb{Z}_S)$  if

$$(6.30) \quad 2^8 \cdot p < 350000$$

or  $p \leq 1367$ . It follows that except for  $p = 5, 7, 17, 31, 257$ , we have

$$(6.31) \quad Y(\mathbb{Z}_S) = Y(\mathbb{Z}_{\{2\}}) = \{(2 : 1), (1 : -1), (1 : 2)\}.$$

In fact, this case is less interesting since computation of  $Y(\mathbb{Z}_S)$  reduces to

$$(6.32) \quad 2^m - p^n = \pm 1,$$

which is a special case of Catalan's equation. Since Catalan's conjecture is known, solutions of the above equation necessarily satisfy  $n = 1$ , and  $Y(\mathbb{Z}_S)$  has more than three elements if and only if  $p$  is a prime of the form  $2^m \pm 1$ . Thus, we are merely verifying Catalan's conjecture.

As another example, take

$$(6.33) \quad S = \{2, 3, p\}$$

consisting of 2, 3 and another prime  $p > 3$ . Since

$$(6.34) \quad \frac{350000}{2^8 \cdot 3} < 456$$

one can use Cremona’s database for primes  $p$  up to 449, which is the 87th prime number. In the next table we display

$$p : m$$

as  $p$  varies among the primes from 5 to 449, and  $Y(\mathbb{Z}_S)$  has  $3 + 6m$  solutions.

5 : 16	7 : 12	11 : 9	13 : 8	17 : 8	19 : 7	23 : 6	29 : 5	31 : 5
37 : 5	41 : 5	43 : 5	47 : 5	53 : 4	59 : 4	61 : 5	67 : 4	71 : 4
73 : 6	79 : 4	83 : 4	89 : 4	97 : 5	101 : 4	103 : 3	107 : 4	109 : 4
113 : 4	127 : 4	131 : 4	137 : 4	139 : 4	149 : 3	151 : 3	157 : 3	163 : 4
167 : 3	173 : 3	179 : 4	181 : 3	191 : 4	193 : 4	197 : 3	199 : 3	211 : 4
223 : 3	227 : 4	229 : 4	233 : 3	239 : 4	241 : 4	251 : 4	257 : 4	263 : 3
269 : 4	271 : 3	277 : 3	281 : 3	283 : 4	293 : 3	307 : 4	311 : 3	313 : 3
317 : 3	331 : 3	337 : 4	347 : 3	349 : 3	353 : 3	359 : 3	367 : 3	373 : 3
379 : 3	383 : 4	389 : 3	397 : 3	401 : 3	409 : 3	419 : 3	421 : 3	431 : 5
433 : 4	439 : 3	443 : 3	449 : 3	//	//	//	//	//

Note that for  $S = \{2, 3\}$ ,  $Y(\mathbb{Z}_S)$  has 21 elements, so in particular  $m = 3$ . The above table indicates that  $m$  stabilises around 3, with a notable exception for  $p = 431$ . It is mainly due to a rather surprising identity  $431 = 2^9 - 3^4$ .

Now we take

$$(6.35) \quad S = \{2, 3, 5, p\}$$

where  $p$  is a prime number which does not exceed 89. Note that  $Y_{\{2,3,5\}}$  contains  $99 = 3 + 6 \times 16$  elements, so a trivial lower bound for  $m$  in this case is 16. Using our algorithm, we obtain the following table:

7 : 62	11 : 46	13 : 44	17 : 37	19 : 37	23 : 35	29 : 31	31 : 30	37 : 30	41 : 30	43 : 28
47 : 26	53 : 28	59 : 25	61 : 26	67 : 26	71 : 25	73 : 25	79 : 25	83 : 25	89 : 23	//

It indicates that  $Y(\mathbb{Z}_S)$  steadily decreases as  $p$  increases, although it is unclear whether it will reach  $m = 16$  at some point. Note an exceptional increment at  $p = 53$ , for which we record the solutions and associated Cremona label in Table 8.3. In fact, the number of possible elliptic curves tends to decrease as  $p$  increases. For example, if  $p = 7$ , there are 1688 curves, while the corresponding number is 1080 for  $p = 87$ .

One wonders whether one can improve the bound on the cardinality of  $Y(\mathbb{Z}_S)$ , as  $S$  varies among certain subsets of prime numbers with fixed cardinality, such as  $S = S_0 \cup \{p\}$  with varying  $p$ .

### 7. COMPARISON WITH THE WORK OF TZANAKIS AND DE WEGER

There has been an attempt to explicitly solve Thue-Mahler equations by Tzanakis and de Weger, based on linear forms in logarithms. Theoretical foundations for the two approaches are quite different, and in this section we compare the two from a practical point of view.

In our approach, the computation of  $\kappa^{-1}(E)$  for a given  $E$  is easy. There is a formula for  $J_6(x, y, h, E)$  to which we plug in the coefficients of  $E$ , and the rational solutions of  $J_6(x, y, h, E)$  can be found quickly. On the other hand, finding all

possible candidates for  $E$  is difficult, although the modularity of elliptic curves significantly facilitates it. The upshot is that in our approach, the modularity of elliptic curves reduces the determination of all possible elliptic curves to a single linear algebra problem on the space of modular forms. One can model the space of modular forms using the space of modular symbols. As Cremona explains in Section 2 of his article [8], computation of modular symbols of a given level can be done rather quickly. On this  $\mathbb{Q}$ -vector space of modular symbols, whose dimension is quite large, one has to find all one-dimensional Hecke invariant rational subspaces and compute sufficiently many Hecke eigenvalues in order to find approximated  $c_4$  and  $c_6$  invariants of a curve in the corresponding isogeny class. Given an isogeny class, it is not so difficult to determine all isomorphism classes which belong to it. To summarise, this linear algebra problem on a huge space of modular symbols seems to lie at the bottleneck of our process.

The approach of Tzanakis and de Weger, as explained in the introduction of [14], consists of three steps. The first is to obtain large bounds from an estimation of linear forms in logarithms of possibly irrational algebraic numbers. The second is to reduce the large bounds using the LLL lattice basis reduction algorithm. The last step is to search for solutions below the bound, not by brute force, but by using an algorithm to search for lattice points on a given sphere, a sieving process, and enumeration of possibilities. The authors remark that the third process might well be the computational bottleneck for their process. They worked out the two following concrete examples:

$$(7.1) \quad x^3 - 23x^2y + 5xy^2 + 24y^3 = \pm 2^{e_1} 3^{e_2} 5^{e_3} 7^{e_4}, \quad \delta = 5^2 \cdot 44621,$$

$$(7.2) \quad x^3 - 3xy^2 - y^3 = \pm 3^{e_1} 17^{e_2} 19^{e_3}, \quad \delta = 3^4,$$

using their method. In order to solve the above equations using our method, we need elliptic curves with conductors dividing  $2^8 \cdot 3 \cdot 5^2 \cdot 7 \cdot 44621^2 > 5 \times 10^{13}$  and  $2^8 \cdot 3^5 \cdot 17 \cdot 19 > 2 \times 10^7$ , which are not provided by Cremona's database.

We observe that the tools of our method have little to do with those of Tzanakis and de Weger. The computational bottlenecks of the two approaches are different: ours is in linear algebra while theirs (seems to) be in the geometry of numbers. As we vary  $h(x, y)$ , we observe another difference. The computations we need to carry out are mostly insensitive to  $h(x, y)$  except for the discriminant and  $S$ . Once the database of elliptic curves is established one can use the same data for a different  $h(x, y)$ . The computations of Tzanakis and de Weger depend on the specific  $S$ -unit equation which is sensitive to a chosen zero of  $h(x, y)$ .

## 8. GENERALISED RAMANUJAN-NAGELL EQUATIONS

The goal of the current section is twofold. Firstly, we shall consider a special form of  $h(x, y)$  and determine  $Y(\mathbb{Z}_S)$ , from which we deduce the complete set of solutions of certain generalised Ramanujan-Nagell equations. Secondly, we shall analyse the statistical behaviour as we vary  $S$  as  $h(x, y)$  remains fixed.

The equation

$$(8.1) \quad x^2 + 7 = 2^n$$

for integers  $x$  and  $n$  is often called the Ramanujan-Nagell equation in the literature. One can relate it to the Thue-Mahler equation, since if we take

$$(8.2) \quad h(x, y) = (x^2 + dy^2)y,$$

then the solution  $(x, n) = (x_0, n_0)$  of the Ramanujan-Nagell equation leads to the point  $(x, y) = (x_0, 1) \in Y(\mathbb{Z}_S)$  for  $d = 7$  and  $S = \{2\}$ . Conversely we can recover the solutions of the Ramanujan-Nagell equation by computing  $Y(\mathbb{Z}_S)$ . Thus one may consider Thue-Mahler equations for (8.2) as a generalisation of the Ramanujan-Nagell equation with  $h(x, y)$  as in (8.2).

In Table 8.4, we display the elements of  $Y(\mathbb{Z}_S)$  for  $d = 7$  and  $S = \{2, 3, 5, 7\}$ , from which we conclude that

$$(8.3) \quad x^2 + 7 = 2^{e_1} 3^{e_2} 5^{e_3} 7^{e_4}$$

with positive  $x$  has seven solutions corresponding to  $x = 181, 21, 11, 7, 5, 3$  and  $1$ . In Table 8.5, we find that

$$(8.4) \quad x^2 + 7 = 2^{e_1} 7^{e_2} 11^{e_3} 13^{e_4}$$

in positive  $x$  has fourteen solutions corresponding to  $x = 273, 181, 75, 53, 35, 31, 21, 13, 11, 9, 7, 5, 3$ , and  $1$ .

For  $d = -7$  and  $S = \{2, 5, 7, 11\}$ , Table 8.12 shows that we have particularly few solutions. Indeed  $Y(\mathbb{Z}_S)$  has five elements, among which three elements satisfy  $y = 1$ . In particular,

$$(8.5) \quad x^2 - 7 = 2^{e_1} 5^{e_2} 7^{e_3} 11^{e_4}$$

has only one solution  $x = 3$  among positive integers.

As we vary  $S$  for a fixed  $d$ , such that  $-d$  is not a square, we observe a pattern which we describe now. The pattern seems to persist for any such  $d$ , but let us take  $d = 1$  for clarity. In particular, we consider

$$(8.6) \quad h(x, y) = (x^2 + y^2)y$$

in the rest of the present section.

Take  $S = \{2, p\}$ , for a prime  $p \geq 3$ . Let the cardinality of  $Y(\mathbb{Z}_{\{2,p\}})$  be  $m$ . We shall divide it into two cases, depending on whether or not  $-1$  is a quadratic residue modulo  $p$ , and compare the variation of  $m$ . Note that  $Y(\mathbb{Z}_{\{2\}})$  has three elements corresponding to  $x = 0, 1$  and  $-1$ . The table below lists

$p : m$
---------

in the range of  $p$  for which  $-1$  is a quadratic residue, and  $p \leq 113$ :

5 : 15	13 : 9	17 : 9	29 : 7	37 : 5	41 : 7	53 : 5
61 : 5	73 : 5	89 : 5	97 : 5	101 : 5	109 : 3	113 : 7

On the other hand, we observe that

$$(8.8) \quad Y(\mathbb{Z}_{\{2,p\}}) = Y(\mathbb{Z}_{\{2\}})$$

if  $-1$  is quadratic non-residue modulo  $p$  and  $p \leq 113$ .

The different behaviour of the cardinality of  $Y(\mathbb{Z}_S)$  continues when we take  $S = \{2, 3, p\}$ . We can numerically verify that

$$(8.9) \quad Y(\mathbb{Z}_{\{2,3,p\}}) = Y(\mathbb{Z}_{\{2\}})$$

if  $-1$  is quadratic non-residue modulo  $p$  and  $p < 455$ . In contrast, if  $-1$  is a quadratic residue modulo  $p$  and  $p < 455$ , then  $Y(\mathbb{Z}_{\{2,3,p\}})$  is strictly larger than  $Y(\mathbb{Z}_{\{2\}})$  all the time. For instance, for  $p = 449$ ,

$$(8.10) \quad (13^2 + 27^2) \cdot 27 = 24246 = 3 \cdot 3^3 \cdot 449$$

is associated to the curve “172416o1”, and similarly for  $p = 433$ ,

$$(8.11) \quad (17^2 + 12^2) \cdot 12 = 5196 = 2^4 \cdot 3 \cdot 433$$

is associated to the curve “20784e2”. The numerical data suggests that the cardinality of  $Y(\mathbb{Z}_{\{2,3,p\}})$  is exactly five for most of  $p$ .

Now we take  $S = \{2, 5, p\}$ . Note that  $Y(\mathbb{Z}_{\{2,5\}})$  consists of fifteen elements. Based on the previous observation, one might conjecture that  $Y(\mathbb{Z}_{\{2,5,p\}})$  consists of fifteen elements if  $-1$  is a quadratic non-residue modulo  $p$ . However, there is a counterexample for  $p = 139$ . Indeed, one finds that

$$(8.12) \quad (29^2 + 278^2) \cdot 278 = 2 \cdot 5^7 \cdot 139,$$

which is associated to the curve “11120e2”. Among the primes  $5 < p \leq 271$  for which  $-1$  is a quadratic non-residue, we verify that

$$(8.13) \quad Y(\mathbb{Z}_{\{2,5,p\}}) = Y(\mathbb{Z}_{\{2,5\}})$$

holds except  $p = 7, 11, 19, 31, 79, 139, 191$ . In these exceptional cases,  $Y(\mathbb{Z}_{\{2,5,p\}}) - Y(\mathbb{Z}_{\{2,5\}})$  contains four elements when  $p = 7, 11$ , and two elements in the remaining five cases. In contrast, if we take  $S = \{2, 5, p\}$  for a prime  $p$  for which  $-1$  is a quadratic residue, then  $Y(\mathbb{Z}_{\{2,5,p\}})$  is strictly larger than  $Y(\mathbb{Z}_{\{2,5\}})$ , in the range  $5 < p \leq 271$ . The smallest cardinality of  $Y(\mathbb{Z}_{\{2,5,p\}})$  is seventeen, which happens precisely for  $p = 241$ . Up to sign of  $x_t$  there is a unique element of  $Y(\mathbb{Z}_{\{2,5,241\}})$  which does not belong to  $Y(\mathbb{Z}_{\{2,5\}})$ , which is

$$(8.14) \quad (15^2 + 4^2)4 = 964 = 2^2 \cdot 241$$

associated to the curve “15424d2”.

We conclude by formulating a precise question based on our observation. Let  $S_0$  be a fixed set of primes. For a positive real number  $X$  and  $i \in \{1, 3\}$ , let  $\pi_i(X)$  be the number of primes  $p$  less than  $X$  which are congruent to  $i$  modulo 4. Define

$$(8.15) \quad A_1(S_0) = \liminf_{X \rightarrow \infty} \frac{1}{\pi_1(X)} \left( \sum_{p < X, p \equiv 1 \pmod{4}} |Y(\mathbb{Z}_{S_0 \cup \{p\}})| \right)$$

and

$$(8.16) \quad A_3(S_0) = \limsup_{X \rightarrow \infty} \frac{1}{\pi_3(X)} \left( \sum_{p < X, p \equiv 3 \pmod{4}} |Y(\mathbb{Z}_{S_0 \cup \{p\}})| \right).$$

One might speculate that  $A_1(\{2\}) = 5$  and  $A_3(\{2\}) = 3$ . To be on the conservative side, one might ask whether

$$(8.17) \quad A_1(S_0) > A_3(S_0)$$

holds. The author is not able to show that

$$(8.18) \quad A_1(S_0) \geq A_3(S_0)$$

holds for any particular  $S_0$ .

TABLE 8.1.  $(a, b, c, d) = (0, 1, -1, 0)$ ,  $\delta = 1$ ,  $S = \{2, 7, 11, 13\}$

$(-343, 169)$ 29679104 $2^9 \cdot 7^3 \cdot 13^2$ 5824bd2 $2^6 \cdot 7 \cdot 13$	$(-169, 7)$ 208208 $2^4 \cdot 7 \cdot 11 \cdot 13^2$ 64064a2 $2^6 \cdot 7 \cdot 11 \cdot 13$	$(-169, 343)$ 29679104 $2^9 \cdot 7^3 \cdot 13^2$ 5824bd2 $2^6 \cdot 7 \cdot 13$	$(-121, 7)$ 108416 $2^7 \cdot 7 \cdot 11^2$ 4928h2 $2^6 \cdot 7 \cdot 11$	$(-64, 13)$ 64064 $2^6 \cdot 7 \cdot 11 \cdot 13$ 64064k2 $2^6 \cdot 7 \cdot 11 \cdot 13$
$(-13, 1)$ 182 $2 \cdot 7 \cdot 13$ 5824b2 $2^6 \cdot 7 \cdot 13$	$(-13, 64)$ 64064 $2^6 \cdot 7 \cdot 11 \cdot 13$ 64064k2 $2^6 \cdot 7 \cdot 11 \cdot 13$	$(-11, 2)$ 286 $2 \cdot 11 \cdot 13$ 9152bd2 $2^6 \cdot 11 \cdot 13$	$(-7, 1)$ 56 $2^3 \cdot 7$ 448b2 $2^6 \cdot 7$	$(-7, 4)$ 308 $2^2 \cdot 7 \cdot 11$ 4928m2 $2^6 \cdot 7 \cdot 11$
$(-7, 121)$ 108416 $2^7 \cdot 7 \cdot 11^2$ 4928h2 $2^6 \cdot 7 \cdot 11$	$(-7, 169)$ 208208 $2^4 \cdot 7 \cdot 11 \cdot 13^2$ 64064a2 $2^6 \cdot 7 \cdot 11 \cdot 13$	$(-4, 7)$ 308 $2^2 \cdot 7 \cdot 11$ 4928m2 $2^6 \cdot 7 \cdot 11$	$(-2, 11)$ 286 $2 \cdot 11 \cdot 13$ 9152bd2 $2^6 \cdot 11 \cdot 13$	$(-1, 1)$ 2 2 256c2 $2^8$
$(-1, 7)$ 56 $2^3 \cdot 7$ 448b2 $2^6 \cdot 7$	$(-1, 13)$ 182 $2 \cdot 7 \cdot 13$ 5824b2 $2^6 \cdot 7 \cdot 13$	$(1, 2)$ -2 -1 · 2 256c2 $2^8$	$(1, 8)$ -56 $-1 \cdot 2^3 \cdot 7$ 448b2 $2^6 \cdot 7$	$(1, 14)$ -182 $-1 \cdot 2 \cdot 7 \cdot 13$ 5824b2 $2^6 \cdot 7 \cdot 13$
$(2, 1)$ 2 2 256c2 $2^8$	$(2, 13)$ -286 $-1 \cdot 2 \cdot 11 \cdot 13$ 9152bd2 $2^6 \cdot 11 \cdot 13$	$(4, 11)$ -308 $-1 \cdot 2^2 \cdot 7 \cdot 11$ 4928m2 $2^6 \cdot 7 \cdot 11$	$(7, 8)$ -56 $-1 \cdot 2^2 \cdot 7$ 448b2 $2^6 \cdot 7$	$(7, 11)$ -308 $-1 \cdot 2^2 \cdot 7 \cdot 11$ 4928m2 $2^6 \cdot 7 \cdot 11$
$(7, 128)$ -108416 $-1 \cdot 2^7 \cdot 7 \cdot 11^2$ 4928h2 $2^6 \cdot 7 \cdot 11$	$(7, 176)$ -208208 $-1 \cdot 2^4 \cdot 7 \cdot 11 \cdot 13^2$ 64064a2 $2^6 \cdot 7 \cdot 11 \cdot 13$	$(8, 1)$ 56 $2^3 \cdot 7$ 448b2 $2^6 \cdot 7$	$(8, 7)$ 56 $2^3 \cdot 7$ 448b2 $2^6 \cdot 7$	$(11, 4)$ 308 $2^2 \cdot 7 \cdot 11$ 4928m2 $2^6 \cdot 7 \cdot 11$
$(11, 7)$ 308 $2^2 \cdot 7 \cdot 11$ 4928m2 $2^6 \cdot 7 \cdot 11$	$(11, 13)$ -286 $-1 \cdot 2 \cdot 11 \cdot 13$ 9152bd2 $2^6 \cdot 11 \cdot 13$	$(13, 2)$ 286 $2 \cdot 11 \cdot 13$ 9152bd2 $2^6 \cdot 11 \cdot 13$	$(13, 11)$ 286 $2 \cdot 11 \cdot 13$ 9152bd2 $2^6 \cdot 11 \cdot 13$	$(13, 14)$ -182 $-1 \cdot 2 \cdot 7 \cdot 13$ 5824b2 $2^6 \cdot 7 \cdot 13$
$(13, 77)$ -64064 $-1 \cdot 2^6 \cdot 7 \cdot 11 \cdot 13$ 64064k2 $2^6 \cdot 7 \cdot 11 \cdot 13$	$(14, 1)$ 182 $2 \cdot 7 \cdot 13$ 5824b2 $2^6 \cdot 7 \cdot 13$	$(14, 13)$ 182 $2 \cdot 7 \cdot 13$ 5824b2 $2^6 \cdot 7 \cdot 13$	$(64, 77)$ -64064 $-1 \cdot 2^6 \cdot 7 \cdot 11 \cdot 13$ 64064k2 $2^6 \cdot 7 \cdot 11 \cdot 13$	$(77, 13)$ 64064 $2^6 \cdot 7 \cdot 11 \cdot 13$ 64064k2 $2^6 \cdot 7 \cdot 11 \cdot 13$
$(77, 64)$ 64064 $2^6 \cdot 7 \cdot 11 \cdot 13$ 64064k2 $2^6 \cdot 7 \cdot 11 \cdot 13$	$(121, 128)$ -108416 $-1 \cdot 2^7 \cdot 7 \cdot 11^2$ 4928h2 $2^6 \cdot 7 \cdot 11$	$(128, 7)$ 108416 $2^7 \cdot 7 \cdot 11^2$ 4928h2 $2^6 \cdot 7 \cdot 11$	$(128, 121)$ 108416 $2^7 \cdot 7 \cdot 11^2$ 4928h2 $2^6 \cdot 7 \cdot 11$	$(169, 176)$ -208208 $-1 \cdot 2^4 \cdot 7 \cdot 11 \cdot 13^2$ 64064a2 $2^6 \cdot 7 \cdot 11 \cdot 13$
$(169, 512)$ -29679104 $-1 \cdot 2^9 \cdot 7^3 \cdot 13^2$ 5824bd2 $2^6 \cdot 7 \cdot 13$	$(176, 7)$ 208208 $2^4 \cdot 7 \cdot 11 \cdot 13^2$ 64064a2 $2^6 \cdot 7 \cdot 11 \cdot 13$	$(176, 169)$ 208208 $2^4 \cdot 7 \cdot 11 \cdot 13^2$ 64064a2 $2^6 \cdot 7 \cdot 11 \cdot 13$	$(343, 512)$ -29679104 $-1 \cdot 2^9 \cdot 7^3 \cdot 13^2$ 5824bd2 $2^6 \cdot 7 \cdot 13$	$(512, 169)$ 29679104 $2^9 \cdot 7^3 \cdot 13^2$ 5824bd2 $2^6 \cdot 7 \cdot 13$
$(512, 343)$ 29679104 $2^9 \cdot 7^3 \cdot 13^2$ 5824bd2 $2^6 \cdot 7 \cdot 13$	empty	empty	empty	empty

TABLE 8.2.  $(a, b, c, d) = (0, 1, -1, 0)$ ,  $\delta = 1$ ,  $S = \{2, 3, 431\}$ 

$(-431, 1)$ 186192 $2^4 \cdot 3^3 \cdot 431$ 82752bd2 $2^6 \cdot 3 \cdot 431$	$(-431, 81)$ 17874432 $2^9 \cdot 3^4 \cdot 431$ 82752t2 $2^6 \cdot 3 \cdot 431$	$(-81, 431)$ 17874432 $2^9 \cdot 3^4 \cdot 431$ 82752t2 $2^6 \cdot 3 \cdot 431$	$(-8, 1)$ 72 $2^3 \cdot 3^2$ 192c3 $2^6 \cdot 3$	$(-3, 1)$ 12 $2^2 \cdot 3$ 192d2 $2^6 \cdot 3$	$(-2, 1)$ 6 $2 \cdot 3$ 192b2 $2^6 \cdot 3$
$(-1, 1)$ 2 2 256c2 $2^8$	$(-1, 2)$ 6 $2 \cdot 3$ 192b2 $2^6 \cdot 3$	$(-1, 3)$ 12 $2^2 \cdot 3$ 192d2 $2^6 \cdot 3$	$(-1, 8)$ 72 $2^3 \cdot 3^2$ 192c3 $2^6 \cdot 3$	$(-1, 431)$ 186192 $2^4 \cdot 3^3 \cdot 431$ 82752bd2 $2^6 \cdot 3 \cdot 431$	$(1, 2)$ -2 $-1 \cdot 2$ 256c2 $2^8$
$(1, 3)$ -6 $-1 \cdot 2 \cdot 3$ 192b2 $2^6 \cdot 3$	$(1, 4)$ -12 $-1 \cdot 2^2 \cdot 3$ 192d2 $2^6 \cdot 3$	$(1, 9)$ -72 $-1 \cdot 2^3 \cdot 3^2$ 192c3 $2^6 \cdot 3$	$(1, 432)$ -186192 $-1 \cdot 2^4 \cdot 3^3 \cdot 431$ 82752bd2 $2^6 \cdot 3 \cdot 431$	$(2, 1)$ 2 2 256c2 $2^8$	$(2, 3)$ -6 $-1 \cdot 2 \cdot 3$ 192b2 $2^6 \cdot 3$
$(3, 1)$ 6 $2 \cdot 3$ 192b2 $2^6 \cdot 3$	$(3, 2)$ 6 $2 \cdot 3$ 192b2 $2^6 \cdot 3$	$(3, 4)$ -12 $-1 \cdot 2^2 \cdot 3$ 192d2 $2^6 \cdot 3$	$(4, 1)$ 12 $2^2 \cdot 3$ 192d2 $2^6 \cdot 3$	$(4, 3)$ 12 $2^2 \cdot 3$ 192d2 $2^6 \cdot 3$	$(8, 9)$ -72 $-1 \cdot 2^3 \cdot 3^2$ 192c3 $2^6 \cdot 3$
$(9, 1)$ 72 $2^3 \cdot 3^2$ 192c3 $2^6 \cdot 3$	$(9, 8)$ 72 $2^3 \cdot 3^2$ 192c3 $2^6 \cdot 3$	$(81, 512)$ -17874432 $-1 \cdot 2^9 \cdot 3^4 \cdot 431$ 82752t2 $2^6 \cdot 3 \cdot 431$	$(431, 432)$ -186192 $-1 \cdot 2^4 \cdot 3^3 \cdot 431$ 82752bd2 $2^6 \cdot 3 \cdot 431$	$(431, 512)$ -17874432 $-1 \cdot 2^9 \cdot 3^4 \cdot 431$ 82752t2 $2^6 \cdot 3 \cdot 431$	$(432, 1)$ 186192 $2^4 \cdot 3^3 \cdot 431$ 82752bd2 $2^6 \cdot 3 \cdot 431$
$(432, 431)$ 186192 $2^4 \cdot 3^3 \cdot 431$ 82752bd2 $2^6 \cdot 3 \cdot 431$	$(512, 81)$ 17874432 $2^9 \cdot 3^4 \cdot 431$ 82752t2 $2^6 \cdot 3 \cdot 431$	$(512, 431)$ 17874432 $2^9 \cdot 3^4 \cdot 431$ 82752t2 $2^6 \cdot 3 \cdot 431$	empty	empty	empty

TABLE 8.3.  $(a, b, c, d) = (0, 1, -1, 0)$ ,  $\delta = 1$ ,  $S = \{2, 3, 5, 53\}$

(-6561, 64) 50880cd2	(-3072, 53) 50880bq2	(-256, 9) 50880y2	(-159, 1) 50880bx2	(-125, 3) 960e6	(-81, 25) 50880bw2
(-80, 1) 960g5	(-75, 53) 50880dz2	(-72, 53) 50880bv2	(-64, 6561) 50880cd2	(-53, 1) 10176f2	(-53, 27) 50880s2
(-53, 72) 50880bv2	(-53, 75) 50880dz2	(-53, 3072) 50880bq2	(-50, 3) 50880cw2	(-48, 5) 50880bt2	(-45, 8) 50880ea2
(-27, 5) 960o2	(-27, 53) 50880s2	(-25, 2) 960d2	(-25, 81) 50880bw2	(-24, 1) 960b3	(-16, 9) 960g3
(-15, 1) 960i2	(-9, 1) 960j2	(-9, 16) 960g3	(-9, 256) 50880y2	(-8, 1) 192c3	(-8, 45) 50880ea2
(-5, 1) 960f2	(-5, 3) 960c2	(-5, 4) 960l2	(-5, 27) 960o2	(-5, 48) 50880bt2	(-4, 1) 320b2
(-4, 5) 960l2	(-3, 1) 192d2	(-3, 2) 960n2	(-3, 5) 960c2	(-3, 50) 50880cw2	(-3, 125) 960e6
(-2, 1) 192b2	(-2, 3) 960n2	(-2, 25) 960d2	(-1, 1) 256c2	(-1, 2) 192b2	(-1, 3) 192d2
(-1, 4) 320b2	(-1, 5) 960f2	(-1, 8) 192c3	(-1, 9) 960j2	(-1, 15) 960i2	(-1, 24) 960b3
(-1, 53) 10176f2	(-1, 80) 960g5	(-1, 159) 50880bx2	(1, 2) 256c2	(1, 3) 192b2	(1, 4) 192d2
(1, 5) 320b2	(1, 6) 960f2	(1, 9) 192c3	(1, 10) 960j2	(1, 16) 960i2	(1, 25) 960b3
(1, 54) 10176f2	(1, 81) 960g5	(1, 160) 50880bx2	(2, 1) 256c2	(2, 3) 192b2	(2, 5) 960n2
(2, 27) 960d2	(3, 1) 192b2	(3, 2) 192b2	(3, 4) 192d2	(3, 5) 960n2	(3, 8) 960c2
(3, 53) 50880cw2	(3, 128) 960e6	(4, 1) 192d2	(4, 3) 192d2	(4, 5) 320b2	(4, 9) 960l2
(5, 1) 320b2	(5, 2) 960n2	(5, 3) 960n2	(5, 4) 320b2	(5, 6) 960f2	(5, 8) 960c2
(5, 9) 960l2	(5, 32) 960o2	(5, 53) 50880bt2	(6, 1) 960f2	(6, 5) 960f2	(8, 3) 960c2
(8, 5) 960c2	(8, 9) 192c3	(8, 53) 50880ea2	(9, 1) 192c3	(9, 4) 960l2	(9, 5) 960l2
(9, 8) 192c3	(9, 10) 960j2	(9, 25) 960g3	(9, 265) 50880y2	(10, 1) 960j2	(10, 9) 960j2
(15, 16) 960i2	(16, 1) 960i2	(16, 15) 960i2	(16, 25) 960g3	(24, 25) 960b3	(25, 1) 960b3
(25, 9) 960g3	(25, 16) 960g3	(25, 24) 960b3	(25, 27) 960d2	(25, 106) 50880bw2	(27, 2) 960d2
(27, 25) 960d2	(27, 32) 960o2	(27, 80) 50880s2	(32, 5) 960o2	(32, 27) 960o2	(45, 53) 50880ea2
(48, 53) 50880bt2	(50, 53) 50880cw2	(53, 3) 50880cw2	(53, 5) 50880bt2	(53, 8) 50880ea2	(53, 45) 50880ea2
(53, 48) 50880bt2	(53, 50) 50880cw2	(53, 54) 10176f2	(53, 80) 50880s2	(53, 125) 50880bv2	(53, 128) 50880dz2
(53, 3125) 50880bq2	(54, 1) 10176f2	(54, 53) 10176f2	(64, 6625) 50880cd2	(72, 125) 50880bv2	(75, 128) 50880dz2
(80, 27) 50880s2	(80, 53) 50880s2	(80, 81) 960g5	(81, 1) 960g5	(81, 80) 960g5	(81, 106) 50880bw2
(106, 25) 50880bw2	(106, 81) 50880bw2	(125, 53) 50880bv2	(125, 72) 50880bv2	(125, 128) 960e6	(128, 3) 960e6
(128, 53) 50880dz2	(128, 75) 50880dz2	(128, 125) 960e6	(159, 160) 50880bx2	(160, 1) 50880bx2	(160, 159) 50880bx2
(256, 265) 50880y2	(265, 9) 50880y2	(265, 256) 50880y2	(3072, 3125) 50880bq2	(3125, 53) 50880bq2	(3125, 3072) 50880bq2
(6561, 6625) 50880cd2	(6625, 64) 50880cd2	(6625, 6561) 50880cd2	empty	empty	empty

TABLE 8.4.  $(a, b, c, d) = (0, 1, 0, 7)$ ,  $\delta = -1 \cdot 2^2 \cdot 7$ ,  $S = \{2, 3, 5, 7\}$ 

(-181, 1) 32768 $2^{15}$ 3136y5 $2^6 \cdot 7^2$	(-119, 5) 71680 $2^{11} \cdot 5 \cdot 7$ 15680v1 $2^6 \cdot 5 \cdot 7^2$	(-47, 45) 737280 $2^{14} \cdot 3^2 \cdot 5$ 210e1 $2 \cdot 3 \cdot 5 \cdot 7$	(-35, 9) 16128 $2^8 \cdot 3^2 \cdot 7$ 294g1 $2 \cdot 3 \cdot 7^2$	(-31, 3) 3072 $2^{10} \cdot 3$ 9408p1 $2^6 \cdot 3 \cdot 7^2$
(-21, 1) 448 $2^6 \cdot 7$ 3136r3 $2^6 \cdot 7^2$	(-13, 7) 3584 $2^9 \cdot 7$ 14a1 $2 \cdot 7$	(-11, 1) 128 $2^7$ 3136k1 $2^6 \cdot 7^2$	(-9, 5) 1280 $2^8 \cdot 5$ 70a1 $2 \cdot 5 \cdot 7$	(-7, 1) 56 $2^3 \cdot 7$ 3136h1 $2^6 \cdot 7^2$
(-7, 3) 336 $2^4 \cdot 3 \cdot 7$ 2352g1 $2^4 \cdot 3 \cdot 7^2$	(-7, 5) 1120 $2^5 \cdot 5 \cdot 7$ 3920o1 $2^4 \cdot 5 \cdot 7^2$	(-5, 1) 32 $2^5$ 3136bb1 $2^6 \cdot 7^2$	(-3, 1) 16 $2^4$ 112b1 $2^4 \cdot 7$	(-1, 1) 8 $2^3$ 224a1 $2^5 \cdot 7$
(-1, 3) 192 $2^6 \cdot 3$ 21a4 $3 \cdot 7$	(0, 1) 7 7 12544a2 $2^8 \cdot 7^2$	(1, 1) 8 $2^3$ 224a1 $2^5 \cdot 7$	(1, 3) 192 $2^6 \cdot 3$ 21a4 $3 \cdot 7$	(3, 1) 16 $2^4$ 112b1 $2^4 \cdot 7$
(5, 1) 32 $2^5$ 3136bb1 $2^6 \cdot 7^2$	(7, 1) 56 $2^3 \cdot 7$ 3136h1 $2^6 \cdot 7^2$	(7, 3) 336 $2^4 \cdot 3 \cdot 7$ 2352g1 $2^4 \cdot 3 \cdot 7^2$	(7, 5) 1120 $2^5 \cdot 5 \cdot 7$ 3920o1 $2^4 \cdot 5 \cdot 7^2$	(9, 5) 1280 $2^8 \cdot 5$ 70a1 $2 \cdot 5 \cdot 7$
(11, 1) 128 $2^7$ 3136k1 $2^6 \cdot 7^2$	(13, 7) 3584 $2^9 \cdot 7$ 14a1 $2 \cdot 7$	(21, 1) 448 $2^6 \cdot 7$ 3136r3 $2^6 \cdot 7^2$	(31, 3) 3072 $2^{10} \cdot 3$ 9408p1 $2^6 \cdot 3 \cdot 7^2$	(35, 9) 16128 $2^8 \cdot 3^2 \cdot 7$ 294g1 $2 \cdot 3 \cdot 7^2$
(47, 45) 737280 $2^{14} \cdot 3^2 \cdot 5$ 210e1 $2 \cdot 3 \cdot 5 \cdot 7$	(119, 5) 71680 $2^{11} \cdot 5 \cdot 7$ 15680v1 $2^6 \cdot 5 \cdot 7^2$	(181, 1) 32768 $2^{15}$ 3136y5 $2^6 \cdot 7^2$	empty	empty

TABLE 8.5.  $(a, b, c, d) = (0, 1, 0, 7)$ ,  $\delta = -1 \cdot 2^2 \cdot 7$ ,  $S = \{2, 7, 11, 13\}$

(-273, 1) 74536 $2^3 \cdot 7 \cdot 11^3$ 34496dc1 $2^6 \cdot 7^2 \cdot 11$	(-181, 1) 32768 $2^{15}$ 3136y5 $2^6 \cdot 7^2$	(-161, 13) 352352 $2^5 \cdot 7 \cdot 11^2 \cdot 13$ 112112o1 $2^4 \cdot 7^2 \cdot 11 \cdot 13$	(-87, 91) 5963776 $2^{16} \cdot 7 \cdot 13$ 182a1 $2 \cdot 7 \cdot 13$	(-81, 13) 100672 $2^6 \cdot 11^2 \cdot 13$ 112112bf1 $2^4 \cdot 7^2 \cdot 11 \cdot 13$	(-75, 1) 5632 $2^9 \cdot 11$ 34496bf1 $2^6 \cdot 7^2 \cdot 11$
(-67, 49) 1043504 $2^4 \cdot 7^2 \cdot 11^3$ 1232d1 $2^4 \cdot 7 \cdot 11$	(-57, 11) 45056 $2^{12} \cdot 11$ 34496cf1 $2^6 \cdot 7^2 \cdot 11$	(-53, 1) 2816 $2^8 \cdot 11$ 34496do1 $2^6 \cdot 7^2 \cdot 11$	(-49, 13) 46592 $2^9 \cdot 7 \cdot 13$ 1274j1 $2 \cdot 7^2 \cdot 13$	(-35, 1) 1232 $2^4 \cdot 7 \cdot 11$ 34496z1 $2^6 \cdot 7^2 \cdot 11$	(-31, 1) 968 $2^3 \cdot 11^2$ 34496dj1 $2^6 \cdot 7^2 \cdot 11$
(-25, 7) 6776 $2^3 \cdot 7 \cdot 11^2$ 2464d1 $2^5 \cdot 7 \cdot 11$	(-21, 1) 448 $2^6 \cdot 7$ 3136r3 $2^6 \cdot 7^2$	(-19, 7) 4928 $2^6 \cdot 7 \cdot 11$ 77c1 $7 \cdot 11$	(-15, 13) 18304 $2^7 \cdot 11 \cdot 13$ 2002c1 $2 \cdot 7 \cdot 11 \cdot 13$	(-13, 1) 176 $2^4 \cdot 11$ 34496cs1 $2^6 \cdot 7^2 \cdot 11$	(-13, 7) 3584 $2^9 \cdot 7$ 14a1 $2 \cdot 7$
(-11, 1) 128 $2^7$ 3136k1 $2^6 \cdot 7^2$	(-9, 1) 88 $2^3 \cdot 11$ 34496bb1 $2^6 \cdot 7^2 \cdot 11$	(-7, 1) 56 $2^3 \cdot 7$ 3136h1 $2^6 \cdot 7^2$	(-7, 2) 154 $2 \cdot 7 \cdot 11$ 8624h2 $2^4 \cdot 7^2 \cdot 11$	(-7, 11) 9856 $2^7 \cdot 7 \cdot 11$ 1078l1 $2 \cdot 7^2 \cdot 11$	(-7, 13) 16016 $2^4 \cdot 7 \cdot 11 \cdot 13$ 112112i1 $2^4 \cdot 7^2 \cdot 11 \cdot 13$
(-5, 1) 32 $2^5$ 3136bb1 $2^6 \cdot 7^2$	(-3, 1) 16 $2^4$ 112b1 $2^4 \cdot 7$	(-3, 4) 484 $2^2 \cdot 11^2$ 616e4 $2^3 \cdot 7 \cdot 11$	(-3, 7) 2464 $2^5 \cdot 7 \cdot 11$ 1232e1 $2^4 \cdot 7 \cdot 11$	(-2, 1) 11 11 2464k1 $2^5 \cdot 7 \cdot 11$	(-1, 1) 8 $2^3$ 224a1 $2^5 \cdot 7$
(0, 1) 7 7 12544a2 $2^8 \cdot 7^2$	(1, 1) 8 $2^3$ 224a1 $2^5 \cdot 7$	(2, 1) 11 11 2464k1 $2^5 \cdot 7 \cdot 11$	(3, 1) 16 $2^4$ 112b1 $2^4 \cdot 7$	(3, 4) 484 $2^2 \cdot 11^2$ 616e4 $2^3 \cdot 7 \cdot 11$	(3, 7) 2464 $2^5 \cdot 7 \cdot 11$ 1232e1 $2^4 \cdot 7 \cdot 11$
(5, 1) 32 $2^5$ 3136bb1 $2^6 \cdot 7^2$	(7, 1) 56 $2^3 \cdot 7$ 3136h1 $2^6 \cdot 7^2$	(7, 2) 154 $2 \cdot 7 \cdot 11$ 8624h2 $2^4 \cdot 7^2 \cdot 11$	(7, 11) 9856 $2^7 \cdot 7 \cdot 11$ 1078l1 $2 \cdot 7^2 \cdot 11$	(7, 13) 16016 $2^4 \cdot 7 \cdot 11 \cdot 13$ 112112i1 $2^4 \cdot 7^2 \cdot 11 \cdot 13$	(9, 1) 88 $2^3 \cdot 11$ 34496bb1 $2^6 \cdot 7^2 \cdot 11$
(11, 1) 128 $2^7$ 3136k1 $2^6 \cdot 7^2$	(13, 1) 176 $2^4 \cdot 11$ 34496cs1 $2^6 \cdot 7^2 \cdot 11$	(13, 7) 3584 $2^9 \cdot 7$ 14a1 $2 \cdot 7$	(15, 13) 18304 $2^7 \cdot 11 \cdot 13$ 2002c1 $2 \cdot 7 \cdot 11 \cdot 13$	(19, 7) 4928 $2^6 \cdot 7 \cdot 11$ 77c1 $7 \cdot 11$	(21, 1) 448 $2^6 \cdot 7$ 3136r3 $2^6 \cdot 7^2$
(25, 7) 6776 $2^3 \cdot 7 \cdot 11^2$ 2464d1 $2^5 \cdot 7 \cdot 11$	(31, 1) 968 $2^3 \cdot 11^2$ 34496dj1 $2^6 \cdot 7^2 \cdot 11$	(35, 1) 1232 $2^4 \cdot 7 \cdot 11$ 34496z1 $2^6 \cdot 7^2 \cdot 11$	(49, 13) 46592 $2^9 \cdot 7 \cdot 13$ 1274j1 $2 \cdot 7^2 \cdot 13$	(53, 1) 2816 $2^8 \cdot 11$ 34496do1 $2^6 \cdot 7^2 \cdot 11$	(57, 11) 45056 $2^{12} \cdot 11$ 34496cf1 $2^6 \cdot 7^2 \cdot 11$
(67, 49) 1043504 $2^4 \cdot 7^2 \cdot 11^3$ 1232d1 $2^4 \cdot 7 \cdot 11$	(75, 1) 5632 $2^9 \cdot 11$ 34496bf1 $2^6 \cdot 7^2 \cdot 11$	(81, 13) 100672 $2^6 \cdot 11^2 \cdot 13$ 112112bf1 $2^4 \cdot 7^2 \cdot 11 \cdot 13$	(87, 91) 5963776 $2^{16} \cdot 7 \cdot 13$ 182a1 $2 \cdot 7 \cdot 13$	(161, 13) 352352 $2^5 \cdot 7 \cdot 11^2 \cdot 13$ 112112o1 $2^4 \cdot 7^2 \cdot 11 \cdot 13$	(181, 1) 32768 $2^{15}$ 3136y5 $2^6 \cdot 7^2$
(273, 1) 74536 $2^3 \cdot 7 \cdot 11^3$ 34496dc1 $2^6 \cdot 7^2 \cdot 11$	empty	empty	empty	empty	empty

TABLE 8.6.  $(a, b, c, d) = (0, 1, 0, 2)$ ,  $\delta = -1 \cdot 2^3$ ,  $S = \{2, 3, 11\}$ 

(-695, 8) 3865224 $2^3 \cdot 3 \cdot 11^5$ 2112d4 $2^6 \cdot 3 \cdot 11$	(-241, 22) 1299078 $2 \cdot 3^{10} \cdot 11$ 2112n4 $2^6 \cdot 3 \cdot 11$	(-155, 4) 96228 $2^2 \cdot 3^7 \cdot 11$ 2112j2 $2^6 \cdot 3 \cdot 11$	(-140, 1) 19602 $2 \cdot 3^4 \cdot 11^2$ 8448e2 $2^8 \cdot 3 \cdot 11$	(-59, 16) 63888 $2^4 \cdot 3 \cdot 11^3$ 2112e4 $2^6 \cdot 3 \cdot 11$	(-50, 9) 23958 $2 \cdot 3^2 \cdot 11^3$ 8448q2 $2^8 \cdot 3 \cdot 11$
(-31, 8) 8712 $2^3 \cdot 3^2 \cdot 11^2$ 2112r4 $2^6 \cdot 3 \cdot 11$	(-25, 32) 85536 $2^5 \cdot 3^5 \cdot 11$ 66c2 $2 \cdot 3 \cdot 11$	(-22, 1) 486 $2 \cdot 3^5$ 768d4 $2^8 \cdot 3$	(-19, 1) 363 $3 \cdot 11^2$ 4224s2 $2^7 \cdot 3 \cdot 11$	(-17, 2) 594 $2 \cdot 3^3 \cdot 11$ 2112b2 $2^6 \cdot 3 \cdot 11$	(-14, 1) 198 $2 \cdot 3^2 \cdot 11$ 8448f2 $2^8 \cdot 3 \cdot 11$
(-13, 8) 2376 $2^3 \cdot 3^3 \cdot 11$ 66a2 $2 \cdot 3 \cdot 11$	(-8, 1) 66 $2 \cdot 3 \cdot 11$ 8448c2 $2^8 \cdot 3 \cdot 11$	(-7, 4) 324 $2^2 \cdot 3^4$ 24a6 $2^3 \cdot 3$	(-7, 6) 726 $2 \cdot 3 \cdot 11^2$ 1056c4 $2^5 \cdot 3 \cdot 11$	(-5, 1) 27 $3^3$ 384g2 $2^7 \cdot 3$	(-5, 2) 66 $2 \cdot 3 \cdot 11$ 2112i2 $2^6 \cdot 3 \cdot 11$
(-4, 1) 18 $2 \cdot 3^2$ 768c2 $2^8 \cdot 3$	(-3, 1) 11 11 1408d2 $2^7 \cdot 11$	(-2, 1) 6 $2 \cdot 3$ 768h1 $2^8 \cdot 3$	(-2, 3) 66 $2 \cdot 3 \cdot 11$ 8448t1 $2^8 \cdot 3 \cdot 11$	(-1, 1) 3 3 384b1 $2^7 \cdot 3$	(-1, 2) 18 $2 \cdot 3^2$ 96b4 $2^5 \cdot 3$
(-1, 4) 132 $2^2 \cdot 3 \cdot 11$ 528a2 $2^4 \cdot 3 \cdot 11$	(-1, 11) 2673 $3^5 \cdot 11$ 4224j1 $2^7 \cdot 3 \cdot 11$	(0, 1) 2 2 256c2 $2^8$	(1, 1) 3 3 384b1 $2^7 \cdot 3$	(1, 2) 18 $2 \cdot 3^2$ 96b4 $2^5 \cdot 3$	(1, 4) 132 $2^2 \cdot 3 \cdot 11$ 528a2 $2^4 \cdot 3 \cdot 11$
(1, 11) 2673 $3^5 \cdot 11$ 4224j1 $2^7 \cdot 3 \cdot 11$	(2, 1) 6 $2 \cdot 3$ 768h1 $2^8 \cdot 3$	(2, 3) 66 $2 \cdot 3 \cdot 11$ 8448t1 $2^8 \cdot 3 \cdot 11$	(3, 1) 11 11 1408d2 $2^7 \cdot 11$	(4, 1) 18 $2 \cdot 3^2$ 768c2 $2^8 \cdot 3$	(5, 1) 27 $3^3$ 384g2 $2^7 \cdot 3$
(5, 2) 66 $2 \cdot 3 \cdot 11$ 2112i2 $2^6 \cdot 3 \cdot 11$	(7, 4) 324 $2^2 \cdot 3^4$ 24a6 $2^3 \cdot 3$	(7, 6) 726 $2 \cdot 3 \cdot 11^2$ 1056c4 $2^5 \cdot 3 \cdot 11$	(8, 1) 66 $2 \cdot 3 \cdot 11$ 8448c2 $2^8 \cdot 3 \cdot 11$	(13, 8) 2376 $2^3 \cdot 3^3 \cdot 11$ 66a2 $2 \cdot 3 \cdot 11$	(14, 1) 198 $2 \cdot 3^2 \cdot 11$ 8448f2 $2^8 \cdot 3 \cdot 11$
(17, 2) 594 $2 \cdot 3^3 \cdot 11$ 2112b2 $2^6 \cdot 3 \cdot 11$	(19, 1) 363 $3 \cdot 11^2$ 4224s2 $2^7 \cdot 3 \cdot 11$	(22, 1) 486 $2 \cdot 3^5$ 768d4 $2^8 \cdot 3$	(25, 32) 85536 $2^5 \cdot 3^5 \cdot 11$ 66c2 $2 \cdot 3 \cdot 11$	(31, 8) 8712 $2^3 \cdot 3^2 \cdot 11^2$ 2112r4 $2^6 \cdot 3 \cdot 11$	(50, 9) 23958 $2 \cdot 3^2 \cdot 11^3$ 8448q2 $2^8 \cdot 3 \cdot 11$
(59, 16) 63888 $2^4 \cdot 3 \cdot 11^3$ 2112e4 $2^6 \cdot 3 \cdot 11$	(140, 1) 19602 $2 \cdot 3^4 \cdot 11^2$ 8448e2 $2^8 \cdot 3 \cdot 11$	(155, 4) 96228 $2^2 \cdot 3^7 \cdot 11$ 2112j2 $2^6 \cdot 3 \cdot 11$	(241, 22) 1299078 $2 \cdot 3^{10} \cdot 11$ 2112n4 $2^6 \cdot 3 \cdot 11$	(695, 8) 3865224 $2^3 \cdot 3 \cdot 11^5$ 2112d4 $2^6 \cdot 3 \cdot 11$	empty

TABLE 8.7.  $(a, b, c, d) = (0, 1, 0, 1)$ ,  $\delta = -1 \cdot 2^2$ ,  $S = \{2, 3, 7, 11\}$

$(-1, 1)$	$(0, 1)$	$(1, 1)$
2	1	2
2	1	2
128c1	256c2	128c1
$2^7$	$2^8$	$2^7$

TABLE 8.8.  $(a, b, c, d) = (0, 1, 0, 1)$ ,  $\delta = -1 \cdot 2^2$ ,  $S = \{2, 5, 13\}$

$(-239, 1)$ 57122 $2 \cdot 13^4$ 1664k2 $2^7 \cdot 13$	$(-199, 32)$ 1300000 $2^5 \cdot 5^5 \cdot 13$ 4160i2 $2^6 \cdot 5 \cdot 13$	$(-83, 64)$ 703040 $2^6 \cdot 5 \cdot 13^3$ 130a4 $2 \cdot 5 \cdot 13$	$(-63, 16)$ 67600 $2^4 \cdot 5^2 \cdot 13^2$ 4160a4 $2^6 \cdot 5 \cdot 13$	$(-57, 1)$ 3250 $2 \cdot 5^3 \cdot 13$ 8320d2 $2^7 \cdot 5 \cdot 13$	$(-37, 16)$ 26000 $2^4 \cdot 5^3 \cdot 13$ 4160n2 $2^6 \cdot 5 \cdot 13$
$(-29, 2)$ 1690 $2 \cdot 5 \cdot 13^2$ 4160p2 $2^6 \cdot 5 \cdot 13$	$(-18, 1)$ 325 $5^2 \cdot 13$ 2080b2 $2^5 \cdot 5 \cdot 13$	$(-12, 5)$ 845 $5 \cdot 13^2$ 2080f4 $2^5 \cdot 5 \cdot 13$	$(-11, 2)$ 250 $2 \cdot 5^3$ 320c4 $2^6 \cdot 5$	$(-9, 13)$ 3250 $2 \cdot 5^3 \cdot 13$ 8320a1 $2^7 \cdot 5 \cdot 13$	$(-8, 1)$ 65 $5 \cdot 13$ 2080c2 $2^5 \cdot 5 \cdot 13$
$(-7, 1)$ 50 $2 \cdot 5^2$ 640f2 $2^7 \cdot 5$	$(-7, 4)$ 260 $2^2 \cdot 5 \cdot 13$ 4160c2 $2^6 \cdot 5 \cdot 13$	$(-5, 1)$ 26 $2 \cdot 13$ 1664d2 $2^7 \cdot 13$	$(-3, 1)$ 10 $2 \cdot 5$ 640a2 $2^7 \cdot 5$	$(-3, 2)$ 26 $2 \cdot 13$ 52a1 $2^2 \cdot 13$	$(-3, 4)$ 100 $2^2 \cdot 5^2$ 40a4 $2^3 \cdot 5$
$(-2, 1)$ 5 5 160b2 $2^5 \cdot 5$	$(-1, 1)$ 2 2 128c1 $2^7$	$(-1, 2)$ 10 $2 \cdot 5$ 80b1 $2^4 \cdot 5$	$(-1, 5)$ 130 $2 \cdot 5 \cdot 13$ 8320b1 $2^7 \cdot 5 \cdot 13$	$(-1, 8)$ 520 $2^3 \cdot 5 \cdot 13$ 65a2 $5 \cdot 13$	$(0, 1)$ 1 1 256c2 $2^8$
$(1, 1)$ 2 2 128c1 $2^7$	$(1, 2)$ 10 $2 \cdot 5$ 80b1 $2^4 \cdot 5$	$(1, 5)$ 130 $2 \cdot 5 \cdot 13$ 8320b1 $2^7 \cdot 5 \cdot 13$	$(1, 8)$ 520 $2^3 \cdot 5 \cdot 13$ 65a2 $5 \cdot 13$	$(2, 1)$ 5 5 160b2 $2^5 \cdot 5$	$(3, 1)$ 10 $2 \cdot 5$ 640a2 $2^7 \cdot 5$
$(3, 2)$ 26 $2 \cdot 13$ 52a1 $2^2 \cdot 13$	$(3, 4)$ 100 $2^2 \cdot 5^2$ 40a4 $2^3 \cdot 5$	$(5, 1)$ 26 $2 \cdot 13$ 1664d2 $2^7 \cdot 13$	$(7, 1)$ 50 $2 \cdot 5^2$ 640f2 $2^7 \cdot 5$	$(7, 4)$ 260 $2^2 \cdot 5 \cdot 13$ 4160c2 $2^6 \cdot 5 \cdot 13$	$(8, 1)$ 65 $5 \cdot 13$ 2080c2 $2^5 \cdot 5 \cdot 13$
$(9, 13)$ 3250 $2 \cdot 5^3 \cdot 13$ 8320a1 $2^7 \cdot 5 \cdot 13$	$(11, 2)$ 250 $2 \cdot 5^3$ 320c4 $2^6 \cdot 5$	$(12, 5)$ 845 $5 \cdot 13^2$ 2080f4 $2^5 \cdot 5 \cdot 13$	$(18, 1)$ 325 $5^2 \cdot 13$ 2080b2 $2^5 \cdot 5 \cdot 13$	$(29, 2)$ 1690 $2 \cdot 5 \cdot 13^2$ 4160p2 $2^6 \cdot 5 \cdot 13$	$(37, 16)$ 26000 $2^4 \cdot 5^3 \cdot 13$ 4160n2 $2^6 \cdot 5 \cdot 13$
$(57, 1)$ 3250 $2 \cdot 5^3 \cdot 13$ 8320d2 $2^7 \cdot 5 \cdot 13$	$(63, 16)$ 67600 $2^4 \cdot 5^2 \cdot 13^2$ 4160a4 $2^6 \cdot 5 \cdot 13$	$(83, 64)$ 703040 $2^6 \cdot 5 \cdot 13^3$ 130a4 $2 \cdot 5 \cdot 13$	$(199, 32)$ 1300000 $2^5 \cdot 5^5 \cdot 13$ 4160i2 $2^6 \cdot 5 \cdot 13$	$(239, 1)$ 57122 $2 \cdot 13^4$ 1664k2 $2^7 \cdot 13$	empty

TABLE 8.9.  $(a, b, c, d) = (0, 1, 0, -2)$ ,  $\delta = 2^3$ ,  $S = \{2, 5, 13, 17\}$

(-4855, 3328) 4725284096 $2^8 \cdot 13 \cdot 17^5$ 14144v2 $2^6 \cdot 13 \cdot 17$	(-239, 169) -169 $-1 \cdot 13^2$ 1664h2 $2^7 \cdot 13$	(-71, 8) 39304 $2^3 \cdot 17^3$ 1088c4 $2^6 \cdot 17$	(-37, 26) 442 $2 \cdot 13 \cdot 17$ 14144s2 $2^6 \cdot 13 \cdot 17$	(-33, 20) 5780 $2^2 \cdot 5 \cdot 17^2$ 5440h3 $2^6 \cdot 5 \cdot 17$	(-31, 25) -7225 $-1 \cdot 5^2 \cdot 17^2$ 10880f2 $2^7 \cdot 5 \cdot 17$
(-24, 17) -34 $-1 \cdot 2 \cdot 17$ 4352f2 $2^8 \cdot 17$	(-23, 16) 272 $2^4 \cdot 17$ 1088i2 $2^6 \cdot 17$	(-7, 4) 68 $2^2 \cdot 17$ 1088g2 $2^6 \cdot 17$	(-7, 5) -5 $-1 \cdot 5$ 640d2 $2^7 \cdot 5$	(-7, 13) -3757 $-1 \cdot 13 \cdot 17^2$ 28288f2 $2^7 \cdot 13 \cdot 17$	(-6, 1) 34 $2 \cdot 17$ 4352d2 $2^8 \cdot 17$
(-5, 2) 34 $2 \cdot 17$ 1088j2 $2^6 \cdot 17$	(-4, 5) -170 $-1 \cdot 2 \cdot 5 \cdot 17$ 21760q2 $2^8 \cdot 5 \cdot 17$	(-3, 2) 2 2 64a2 $2^6$	(-2, 1) 2 2 256a2 $2^8$	(-1, 1) -1 -1 128c2 $2^7$	(0, 1) -2 $-1 \cdot 2$ 256c2 $2^8$
(1, 1) -1 -1 128c2 $2^7$	(2, 1) 2 2 256a2 $2^8$	(3, 2) 2 2 64a2 $2^6$	(4, 5) -170 $-1 \cdot 2 \cdot 5 \cdot 17$ 21760q2 $2^8 \cdot 5 \cdot 17$	(5, 2) 34 $2 \cdot 17$ 1088j2 $2^6 \cdot 17$	(6, 1) 34 $2 \cdot 17$ 4352d2 $2^8 \cdot 17$
(7, 4) 68 $2^2 \cdot 17$ 1088g2 $2^6 \cdot 17$	(7, 5) -5 $-1 \cdot 5$ 640d2 $2^7 \cdot 5$	(7, 13) -3757 $-1 \cdot 13 \cdot 17^2$ 28288f2 $2^7 \cdot 13 \cdot 17$	(23, 16) 272 $2^4 \cdot 17$ 1088i2 $2^6 \cdot 17$	(24, 17) -34 $-1 \cdot 2 \cdot 17$ 4352f2 $2^8 \cdot 17$	(31, 25) -7225 $-1 \cdot 5^2 \cdot 17^2$ 10880f2 $2^7 \cdot 5 \cdot 17$
(33, 20) 5780 $2^2 \cdot 5 \cdot 17^2$ 5440h3 $2^6 \cdot 5 \cdot 17$	(37, 26) 442 $2 \cdot 13 \cdot 17$ 14144s2 $2^6 \cdot 13 \cdot 17$	(71, 8) 39304 $2^3 \cdot 17^3$ 1088c4 $2^6 \cdot 17$	(239, 169) -169 $-1 \cdot 13^2$ 1664h2 $2^7 \cdot 13$	(4855, 3328) 4725284096 $2^8 \cdot 13 \cdot 17^5$ 14144v2 $2^6 \cdot 13 \cdot 17$	empty

TABLE 8.10.  $(a, b, c, d) = (0, 1, 0, -2)$ ,  $\delta = 2^3$ ,  $S = \{2, 7, 29\}$

(-181, 128) -896 $-1 \cdot 2^7 \cdot 7$ 448c6 $2^6 \cdot 7$	(-163, 116) -39788 $-1 \cdot 2^2 \cdot 7^3 \cdot 29$ 12992bc2 $2^6 \cdot 7 \cdot 29$	(-45, 29) 9947 $7^3 \cdot 29$ 25984i2 $2^7 \cdot 7 \cdot 29$	(-41, 29) -29 $-1 \cdot 29$ 3712p2 $2^7 \cdot 29$	(-13, 16) -5488 $-1 \cdot 2^4 \cdot 7^3$ 448c4 $2^6 \cdot 7$	(-11, 8) -56 $-1 \cdot 2^3 \cdot 7$ 448f2 $2^6 \cdot 7$
(-10, 1) 98 $2 \cdot 7^2$ 1792f2 $2^8 \cdot 7$	(-10, 7) 14 $2 \cdot 7$ 1792a2 $2^8 \cdot 7$	(-9, 4) 196 $2^2 \cdot 7^2$ 448a3 $2^6 \cdot 7$	(-5, 4) -28 $-1 \cdot 2^2 \cdot 7$ 448h2 $2^6 \cdot 7$	(-4, 1) 14 $2 \cdot 7$ 1792e2 $2^8 \cdot 7$	(-3, 1) 7 7 896d2 $2^7 \cdot 7$
(-3, 2) 2 2 64a2 $2^6$	(-2, 1) 2 2 256a2 $2^8$	(-1, 1) -1 -1 128c2 $2^7$	(-1, 2) -14 $-1 \cdot 2 \cdot 7$ 448d2 $2^6 \cdot 7$	(0, 1) -2 $-1 \cdot 2$ 256c2 $2^8$	(1, 1) -1 -1 128c2 $2^7$
(1, 2) -14 $-1 \cdot 2 \cdot 7$ 448d2 $2^6 \cdot 7$	(2, 1) 2 2 256a2 $2^8$	(3, 1) 7 7 896d2 $2^7 \cdot 7$	(3, 2) 2 2 64a2 $2^6$	(4, 1) 14 $2 \cdot 7$ 1792e2 $2^8 \cdot 7$	(5, 4) -28 $-1 \cdot 2^2 \cdot 7$ 448h2 $2^6 \cdot 7$
(9, 4) 196 $2^2 \cdot 7^2$ 448a3 $2^6 \cdot 7$	(10, 1) 98 $2 \cdot 7^2$ 1792f2 $2^8 \cdot 7$	(10, 7) 14 $2 \cdot 7$ 1792a2 $2^8 \cdot 7$	(11, 8) -56 $-1 \cdot 2^3 \cdot 7$ 448f2 $2^6 \cdot 7$	(13, 16) -5488 $-1 \cdot 2^4 \cdot 7^3$ 448c4 $2^6 \cdot 7$	(41, 29) -29 $-1 \cdot 29$ 3712p2 $2^7 \cdot 29$
(45, 29) 9947 $7^3 \cdot 29$ 25984i2 $2^7 \cdot 7 \cdot 29$	(163, 116) -39788 $-1 \cdot 2^2 \cdot 7^3 \cdot 29$ 12992bc2 $2^6 \cdot 7 \cdot 29$	(181, 128) -896 $-1 \cdot 2^7 \cdot 7$ 448c6 $2^6 \cdot 7$	empty	empty	empty

TABLE 8.11.  $(a, b, c, d) = (0, 1, 0, -3)$ ,  $\delta = 2^2 \cdot 3$ ,  $S = \{2, 3, 7, 11\}$

(-122, 9) 131769 $3^2 \cdot 11^4$ 3168z3 $2^5 \cdot 3^2 \cdot 11$	(-111, 64) 2112 $2^6 \cdot 3 \cdot 11$ 6336b4 $2^6 \cdot 3^2 \cdot 11$	(-97, 56) 56 $2^3 \cdot 7$ 4032bm5 $2^6 \cdot 3^2 \cdot 7$	(-85, 49) 1078 $2 \cdot 7^2 \cdot 11$ 88704z2 $2^7 \cdot 3^2 \cdot 7 \cdot 11$	(-69, 16) 63888 $2^4 \cdot 3 \cdot 11^3$ 6336bi4 $2^6 \cdot 3^2 \cdot 11$	(-53, 7) 18634 $2 \cdot 7 \cdot 11^3$ 88704cs2 $2^7 \cdot 3^2 \cdot 7 \cdot 11$
(-47, 27) 594 $2 \cdot 3^3 \cdot 11$ 12672i2 $2^7 \cdot 3^2 \cdot 11$	(-43, 24) 2904 $2^3 \cdot 3 \cdot 11^2$ 6336bd3 $2^6 \cdot 3^2 \cdot 11$	(-38, 21) 2541 $3 \cdot 7 \cdot 11^2$ 22176f4 $2^5 \cdot 3^2 \cdot 7 \cdot 11$	(-31, 18) -198 $-1 \cdot 2 \cdot 3^2 \cdot 11$ 6336m2 $2^6 \cdot 3^2 \cdot 11$	(-27, 1) 726 $2 \cdot 3 \cdot 11^2$ 12672c2 $2^7 \cdot 3^2 \cdot 11$	(-19, 11) -22 $-1 \cdot 2 \cdot 11$ 12672bc2 $2^7 \cdot 3^2 \cdot 11$
(-15, 8) 264 $2^3 \cdot 3 \cdot 11$ 6336e2 $2^6 \cdot 3^2 \cdot 11$	(-15, 14) -5082 $-1 \cdot 2 \cdot 3 \cdot 7 \cdot 11^2$ 44352c2 $2^6 \cdot 3^2 \cdot 7 \cdot 11$	(-13, 4) 484 $2^2 \cdot 11^2$ 6336ck3 $2^6 \cdot 3^2 \cdot 11$	(-13, 7) 154 $2 \cdot 7 \cdot 11$ 88704be2 $2^7 \cdot 3^2 \cdot 7 \cdot 11$	(-12, 7) -21 $-1 \cdot 3 \cdot 7$ 2016b2 $2^5 \cdot 3^2 \cdot 7$	(-9, 4) 132 $2^2 \cdot 3 \cdot 11$ 6336bh2 $2^6 \cdot 3^2 \cdot 11$
(-9, 7) -462 $-1 \cdot 2 \cdot 3 \cdot 7 \cdot 11$ 88704bk2 $2^7 \cdot 3^2 \cdot 7 \cdot 11$	(-7, 3) 66 $2 \cdot 3 \cdot 11$ 12672m2 $2^7 \cdot 3^2 \cdot 11$	(-7, 4) 4 $2^2$ 576d3 $2^6 \cdot 3^2$	(-6, 1) 33 $3 \cdot 11$ 3168b2 $2^5 \cdot 3^2 \cdot 11$	(-5, 1) 22 $2 \cdot 11$ 12672k2 $2^7 \cdot 3^2 \cdot 11$	(-5, 3) -6 $-1 \cdot 2 \cdot 3$ 1152k2 $2^7 \cdot 3^2$
(-4, 3) -33 $-1 \cdot 3 \cdot 11$ 3168v2 $2^5 \cdot 3^2 \cdot 11$	(-3, 1) 6 $2 \cdot 3$ 1152o2 $2^7 \cdot 3^2$	(-3, 2) -6 $-1 \cdot 2 \cdot 3$ 576a4 $2^6 \cdot 3^2$	(-2, 1) 1 $1$ 288c2 $2^5 \cdot 3^2$	(-1, 1) -2 $-1 \cdot 2$ 1152r2 $2^7 \cdot 3^2$	(-1, 2) -22 $-1 \cdot 2 \cdot 11$ 6336ca2 $2^6 \cdot 3^2 \cdot 11$
(-1, 9) -2178 $-1 \cdot 2 \cdot 3^2 \cdot 11^2$ 12672x2 $2^7 \cdot 3^2 \cdot 11$	(0, 1) -3 $-1 \cdot 3$ 2304j2 $2^8 \cdot 3^2$	(1, 1) -2 $-1 \cdot 2$ 1152r2 $2^7 \cdot 3^2$	(1, 2) -22 $-1 \cdot 2 \cdot 11$ 6336ca2 $2^6 \cdot 3^2 \cdot 11$	(1, 9) -2178 $-1 \cdot 2 \cdot 3^2 \cdot 11^2$ 12672x2 $2^7 \cdot 3^2 \cdot 11$	(2, 1) 1 $1$ 288c2 $2^5 \cdot 3^2$
(3, 1) 6 $2 \cdot 3$ 1152o2 $2^7 \cdot 3^2$	(3, 2) -6 $-1 \cdot 2 \cdot 3$ 576a4 $2^6 \cdot 3^2$	(4, 3) -33 $-1 \cdot 3 \cdot 11$ 3168v2 $2^5 \cdot 3^2 \cdot 11$	(5, 1) 22 $2 \cdot 11$ 12672k2 $2^7 \cdot 3^2 \cdot 11$	(5, 3) -6 $-1 \cdot 2 \cdot 3$ 1152k2 $2^7 \cdot 3^2$	(6, 1) 33 $3 \cdot 11$ 3168b2 $2^5 \cdot 3^2 \cdot 11$
(7, 3) 66 $2 \cdot 3 \cdot 11$ 12672m2 $2^7 \cdot 3^2 \cdot 11$	(7, 4) 4 $2^2$ 576d3 $2^6 \cdot 3^2$	(9, 4) 132 $2^2 \cdot 3 \cdot 11$ 6336bh2 $2^6 \cdot 3^2 \cdot 11$	(9, 7) -462 $-1 \cdot 2 \cdot 3 \cdot 7 \cdot 11$ 88704bk2 $2^7 \cdot 3^2 \cdot 7 \cdot 11$	(12, 7) -21 $-1 \cdot 3 \cdot 7$ 2016b2 $2^5 \cdot 3^2 \cdot 7$	(13, 4) 484 $2^2 \cdot 11^2$ 6336ck3 $2^6 \cdot 3^2 \cdot 11$
(13, 7) 154 $2 \cdot 7 \cdot 11$ 88704be2 $2^7 \cdot 3^2 \cdot 7 \cdot 11$	(15, 8) 264 $2^3 \cdot 3 \cdot 11$ 6336e2 $2^6 \cdot 3^2 \cdot 11$	(15, 14) -5082 $-1 \cdot 2 \cdot 3 \cdot 7 \cdot 11^2$ 44352c2 $2^6 \cdot 3^2 \cdot 7 \cdot 11$	(19, 11) -22 $-1 \cdot 2 \cdot 11$ 12672bc2 $2^7 \cdot 3^2 \cdot 11$	(27, 1) 726 $2 \cdot 3 \cdot 11^2$ 12672c2 $2^7 \cdot 3^2 \cdot 11$	(31, 18) -198 $-1 \cdot 2 \cdot 3^2 \cdot 11$ 6336m2 $2^6 \cdot 3^2 \cdot 11$
(38, 21) 2541 $3 \cdot 7 \cdot 11^2$ 22176f4 $2^5 \cdot 3^2 \cdot 7 \cdot 11$	(43, 24) 2904 $2^3 \cdot 3 \cdot 11^2$ 6336bd3 $2^6 \cdot 3^2 \cdot 11$	(47, 27) 594 $2 \cdot 3^3 \cdot 11$ 12672i2 $2^7 \cdot 3^2 \cdot 11$	(53, 7) 18634 $2 \cdot 7 \cdot 11^3$ 88704cs2 $2^7 \cdot 3^2 \cdot 7 \cdot 11$	(69, 16) 63888 $2^4 \cdot 3 \cdot 11^3$ 6336bi4 $2^6 \cdot 3^2 \cdot 11$	(85, 49) 1078 $2 \cdot 7^2 \cdot 11$ 88704z2 $2^7 \cdot 3^2 \cdot 7 \cdot 11$
(97, 56) 56 $2^3 \cdot 7$ 4032bm5 $2^6 \cdot 3^2 \cdot 7$	(111, 64) 2112 $2^6 \cdot 3 \cdot 11$ 6336b4 $2^6 \cdot 3^2 \cdot 11$	(122, 9) 131769 $3^2 \cdot 11^4$ 3168z3 $2^5 \cdot 3^2 \cdot 11$	empty	empty	empty

TABLE 8.12.  $(a, b, c, d) = (0, 1, 0, -7)$ ,  $\delta = 2^2 \cdot 7$ ,  $S = \{2, 5, 7, 11\}$ 

$(-21, 8)$	$(-3, 1)$	$(0, 1)$	$(3, 1)$	$(21, 8)$
$-56$	$2$	$-7$	$2$	$-56$
$-1 \cdot 2^3 \cdot 7$	$2$	$-1 \cdot 7$	$2$	$-1 \cdot 2^3 \cdot 7$
$3136r4$	$6272b2$	$12544a2$	$6272b2$	$3136r4$
$2^6 \cdot 7^2$	$2^7 \cdot 7^2$	$2^8 \cdot 7^2$	$2^7 \cdot 7^2$	$2^6 \cdot 7^2$

TABLE 8.13.  $(a, b, c, d) = (1, -1, -4, -1)$ ,  $\delta = 13^2$ ,  $S = \{2, 5, 13\}$ 

$(-157, 114)$	$(-43, 157)$	$(-17, 13)$	$(-17, 14)$	$(-11, 8)$	$(-9, 7)$
$65$	$-65$	$625$	$1625$	$5$	$125$
$5 \cdot 13$	$-1 \cdot 5 \cdot 13$	$5^4$	$5^3 \cdot 13$	$5$	$5^3$
$54080bk2$	$54080bk2$	$54080di1$	$54080bk1$	$54080cz1$	$54080bl2$
$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$
$(-7, 5)$	$(-4, 1)$	$(-4, 3)$	$(-4, 17)$	$(-3, 1)$	$(-3, 2)$
$-13$	$-65$	$5$	$-625$	$-25$	$-5$
$-1 \cdot 13$	$-1 \cdot 5 \cdot 13$	$5$	$-1 \cdot 5^4$	$-1 \cdot 5^2$	$-1 \cdot 5$
$10816bi1$	$54080cd1$	$54080cb1$	$54080di1$	$54080dc1$	$54080cx1$
$2^6 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$
$(-3, 4)$	$(-3, 11)$	$(-3, 17)$	$(-2, 1)$	$(-2, 3)$	$(-2, 7)$
$65$	$-5$	$-1625$	$-5$	$25$	$13$
$5 \cdot 13$	$-1 \cdot 5$	$-1 \cdot 5^3 \cdot 13$	$-1 \cdot 5$	$5^2$	$13$
$54080cd1$	$54080cz1$	$54080bk1$	$54080co1$	$54080dc1$	$10816bi1$
$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 13^2$
$(-2, 9)$	$(-1, 1)$	$(-1, 2)$	$(-1, 3)$	$(-1, 4)$	$(0, 1)$
$-125$	$1$	$5$	$5$	$-5$	$-1$
$-1 \cdot 5^3$	$1$	$5$	$5$	$-1 \cdot 5$	$-1$
$54080bl2$	$10816be1$	$54080co1$	$54080cx1$	$54080cb1$	$10816be1$
$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 13^2$
$(1, 1)$	$(1, 2)$	$(1, 3)$	$(2, 1)$	$(3, 1)$	$(5, 2)$
$-5$	$-25$	$-65$	$-5$	$5$	$-13$
$-1 \cdot 5$	$-1 \cdot 5^2$	$-1 \cdot 5 \cdot 13$	$-1 \cdot 5$	$5$	$-1 \cdot 13$
$54080co1$	$54080dc1$	$54080cd1$	$54080cx1$	$54080cb1$	$10816bi1$
$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 13^2$
$(7, 2)$	$(8, 3)$	$(13, 4)$	$(14, 3)$	$(114, 43)$	
$125$	$5$	$625$	$1625$	$65$	
$5^3$	$5$	$5^4$	$5^3 \cdot 13$	$5 \cdot 13$	
$54080bl2$	$54080cz1$	$54080di1$	$54080bk1$	$54080bk2$	empty
$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	$2^6 \cdot 5 \cdot 13^2$	

TABLE 8.14.  $(a, b, c, d) = (1, -1, -2, -2)$ ,  $\delta = -1 \cdot 2^3 \cdot 19$ ,  $S = \{2, 5, 19\}$

$(-81, 13)$ -593750 $-1 \cdot 2 \cdot 5^6 \cdot 19$ 115520ck1 $2^6 \cdot 5 \cdot 19^2$	$(-43, 89)$ -972800 $-1 \cdot 2^{11} \cdot 5^2 \cdot 19$ 3610i1 $2 \cdot 5 \cdot 19^2$	$(-17, 16)$ -9025 $-1 \cdot 5^2 \cdot 19^2$ 12160i1 $2^7 \cdot 5 \cdot 19$	$(-8, 9)$ -1250 $-1 \cdot 2 \cdot 5^4$ 24320s1 $2^8 \cdot 5 \cdot 19$	$(-7, 1)$ -380 $-1 \cdot 2^2 \cdot 5 \cdot 19$ 115520q1 $2^6 \cdot 5 \cdot 19^2$	$(-3, 1)$ -32 $-1 \cdot 2^5$ 23104r1 $2^6 \cdot 19^2$
$(-3, 4)$ -95 $-1 \cdot 5 \cdot 19$ 231040u1 $2^7 \cdot 5 \cdot 19^2$	$(-2, 1)$ -10 $-1 \cdot 2 \cdot 5$ 24320j1 $2^8 \cdot 5 \cdot 19$	$(-2, 3)$ -38 $-1 \cdot 2 \cdot 19$ 4864p1 $2^8 \cdot 19$	$(-1, 1)$ -2 $-1 \cdot 2$ 608f1 $2^5 \cdot 19$	$(-1, 3)$ -40 $-1 \cdot 2^3 \cdot 5$ 190b1 $2 \cdot 5 \cdot 19$	$(-1, 11)$ -2432 $-1 \cdot 2^7 \cdot 19$ 38a1 $2 \cdot 19$
$(0, 1)$ -2 $-1 \cdot 2$ 4864j1 $2^8 \cdot 19$	$(1, 1)$ -4 $-1 \cdot 2^2$ 23104bu1 $2^6 \cdot 19^2$	$(1, 2)$ -25 $-1 \cdot 5^2$ 231040bx1 $2^7 \cdot 5 \cdot 19^2$	$(1, 5)$ -304 $-1 \cdot 2^4 \cdot 19$ 23104bk1 $2^6 \cdot 19^2$	$(2, 1)$ -2 $-1 \cdot 2$ 92416w1 $2^8 \cdot 19^2$	$(3, 1)$ 10 $2 \cdot 5$ 115520bx1 $2^6 \cdot 5 \cdot 19^2$
$(4, 1)$ 38 $2 \cdot 19$ 92416h1 $2^8 \cdot 19^2$	$(5, 2)$ 19 19 46208b1 $2^7 \cdot 19^2$	$(7, 3)$ 16 $2^4$ 2310411 $2^6 \cdot 19^2$	$(9, 29)$ -65536 $-1 \cdot 2^{16}$ 23104bt3 $2^6 \cdot 19^2$	$(11, 7)$ -1280 $-1 \cdot 2^8 \cdot 5$ 115520bh1 $2^6 \cdot 5 \cdot 19^2$	$(13, 1)$ 2000 $2^4 \cdot 5^3$ 115520by1 $2^6 \cdot 5 \cdot 19^2$
$(13, 9)$ -2888 $-1 \cdot 2^3 \cdot 19^2$ 23104bs2 $2^6 \cdot 19^2$	$(16, 7)$ 50 $2 \cdot 5^2$ 24320g1 $2^8 \cdot 5 \cdot 19$	$(17, 9)$ -1900 $-1 \cdot 2^2 \cdot 5^2 \cdot 19$ 115520bm1 $2^6 \cdot 5 \cdot 19^2$	$(18, 11)$ -4750 $-1 \cdot 2 \cdot 5^3 \cdot 19$ 24320p1 $2^8 \cdot 5 \cdot 19$	$(25, 11)$ 38 $2 \cdot 19$ 23104bj1 $2^6 \cdot 19^2$	$(93, 41)$ -760 $-1 \cdot 2^3 \cdot 5 \cdot 19$ 115520by2 $2^6 \cdot 5 \cdot 19^2$
$(376, 177)$ -6516050 $-1 \cdot 2 \cdot 5^2 \cdot 19^4$ 24320h1 $2^8 \cdot 5 \cdot 19$	empty	empty	empty	empty	empty

TABLE 8.15.  $(a, b, c, d) = (1, 0, 0, 1)$ ,  $\delta = -1 \cdot 3^3$ ,  $S = \{2, 3, 5\}$

$(0, 1)$ 1 1 15552b2 $2^6 \cdot 3^5$	$(1, 1)$ 2 2 2304j2 $2^8 \cdot 3^2$	$(1, 2)$ 9 $3^2$ 48a4 $2^4 \cdot 3$	$(2, 1)$ 9 $3^2$ 48a4 $2^4 \cdot 3$	empty	empty
--	---	---	---	-------	-------

TABLE 8.16.  $(a, b, c, d) = (1, 0, 0, 2)$ ,  $\delta = -1 \cdot 2^2 \cdot 3^3$ ,  $S = \{2, 3, 5\}$

$(-37, 29)$ -1875 $-1 \cdot 3 \cdot 5^4$ 4320c1 $2^5 \cdot 3^3 \cdot 5$	$(-5, 4)$ 3 3 432a4 $2^4 \cdot 3^3$	$(-4, 3)$ -10 $-1 \cdot 2 \cdot 5$ 8640cb1 $2^6 \cdot 3^3 \cdot 5$	$(-3, 1)$ -25 $-1 \cdot 5^2$ 4320j1 $2^5 \cdot 3^3 \cdot 5$	$(-2, 1)$ -6 $-1 \cdot 2 \cdot 3$ 1728l1 $2^6 \cdot 3^3$	$(-1, 1)$ 1 1 864i1 $2^5 \cdot 3^3$
$(-1, 2)$ 15 $3 \cdot 5$ 2160w1 $2^4 \cdot 3^3 \cdot 5$	$(0, 1)$ 2 2 15552b2 $2^6 \cdot 3^5$	$(1, 1)$ 3 3 1728h1 $2^6 \cdot 3^3$	$(2, 1)$ 10 $2 \cdot 5$ 1080j1 $2^3 \cdot 3^3 \cdot 5$	$(4, 7)$ 750 $2 \cdot 3 \cdot 5^3$ 540e2 $2^2 \cdot 3^3 \cdot 5$	empty

TABLE 8.17.  $(a, b, c, d) = (1, 0, 0, -2)$ ,  $\delta = -1 \cdot 2^2 \cdot 3^3$ ,  $S = \{2, 3, 5\}$ 

$(-4, 7)$ -750 $-1 \cdot 2 \cdot 3 \cdot 5^3$ 540e2 $2^2 \cdot 3^3 \cdot 5$	$(-2, 1)$ -10 $-1 \cdot 2 \cdot 5$ 1080j1 $2^3 \cdot 3^3 \cdot 5$	$(-1, 1)$ -3 $-1 \cdot 3$ 1728h1 $2^6 \cdot 3^3$	$(0, 1)$ -2 $-1 \cdot 2$ 15552b2 $2^6 \cdot 3^5$	$(1, 1)$ -1 -1 864i1 $2^5 \cdot 3^3$	$(1, 2)$ -15 $-1 \cdot 3 \cdot 5$ 2160w1 $2^4 \cdot 3^3 \cdot 5$
$(2, 1)$ 6 $2 \cdot 3$ 1728l1 $2^6 \cdot 3^3$	$(3, 1)$ 25 $5^2$ 4320j1 $2^5 \cdot 3^3 \cdot 5$	$(4, 3)$ 10 $2 \cdot 5$ 8640cb1 $2^6 \cdot 3^3 \cdot 5$	$(5, 4)$ -3 $-1 \cdot 3$ 432a4 $2^4 \cdot 3^3$	$(37, 29)$ 1875 $3 \cdot 5^4$ 4320c1 $2^5 \cdot 3^3 \cdot 5$	empty

TABLE 8.18.  $(a, b, c, d) = (1, 0, 0, -3)$ ,  $\delta = -1 \cdot 3^5$ ,  $S = \{2, 3, 5\}$ 

$(-21, 17)$ -24000 $-1 \cdot 2^6 \cdot 3 \cdot 5^3$ 2430g1 $2 \cdot 3^5 \cdot 5$	$(-5, 1)$ -128 $-1 \cdot 2^7$ 486a1 $2 \cdot 3^5$	$(-3, 1)$ -30 $-1 \cdot 2 \cdot 3 \cdot 5$ 38880o1 $2^5 \cdot 3^5 \cdot 5$	$(-1, 1)$ -4 $-1 \cdot 2^2$ 1944j1 $2^3 \cdot 3^5$	$(-1, 2)$ -25 $-1 \cdot 5^2$ 19440m1 $2^4 \cdot 3^5 \cdot 5$	$(0, 1)$ -3 $-1 \cdot 3$ 15552b2 $2^6 \cdot 3^5$
$(1, 1)$ -2 $-1 \cdot 2$ 15552k1 $2^6 \cdot 3^5$	$(1, 3)$ -80 $-1 \cdot 2^4 \cdot 5$ 77760q1 $2^6 \cdot 3^5 \cdot 5$	$(2, 1)$ 5 5 77760y1 $2^6 \cdot 3^5 \cdot 5$	$(3, 1)$ 24 $2^3 \cdot 3$ 15552bw1 $2^6 \cdot 3^5$	$(3, 2)$ 3 3 15552bd1 $2^6 \cdot 3^5$	$(7, 5)$ -32 $-1 \cdot 2^5$ 15552bo2 $2^6 \cdot 3^5$
$(9, 7)$ -300 $-1 \cdot 2^2 \cdot 3 \cdot 5^2$ 77760v1 $2^6 \cdot 3^5 \cdot 5$	$(11, 3)$ 1250 $2 \cdot 5^4$ 77760bv1 $2^6 \cdot 3^5 \cdot 5$	$(13, 9)$ 10 $2 \cdot 5$ 77760cs1 $2^6 \cdot 3^5 \cdot 5$	$(33, 19)$ 15360 $2^{10} \cdot 3 \cdot 5$ 77760b2 $2^6 \cdot 3^5 \cdot 5$	empty	empty

## ACKNOWLEDGEMENTS

The author is grateful to the anonymous referee for the careful reading and giving helpful comments. He is also grateful to John Coates and Minhyong Kim for their helpful comments on earlier versions of the paper. This work was supported by IBS-R003-D1.

## REFERENCES

- [1] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, *Canad. J. Math.* **56** (2004), no. 1, 23–54, DOI 10.4153/CJM-2004-002-2. MR2031121 (2005c:11035)
- [2] Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, *Ann. of Math. (2)* **163** (2006), no. 3, 969–1018, DOI 10.4007/annals.2006.163.969. MR2215137 (2007f:11031)
- [3] Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation*, *Compos. Math.* **142** (2006), no. 1, 31–62, DOI 10.1112/S0010437X05001739. MR2196761 (2007f:11032)

- [4] A. Brumer and J. H. Silverman, *The number of elliptic curves over  $\mathbf{Q}$  with conductor  $N$* , *Manuscripta Math.* **91** (1996), no. 1, 95–102, DOI 10.1007/BF02567942. MR1404420 (97e:11062)
- [5] J. Coates, *An effective  $p$ -adic analogue of a theorem of Thue*, *Acta Arith.* **15** (1968/1969), 279–305. MR0242768 (39 #4095)
- [6] J. Coates, *An effective  $p$ -adic analogue of a theorem of Thue. II. The greatest prime factor of a binary form*, *Acta Arith.* **16** (1969/1970), 399–412. MR0263741 (41 #8341)
- [7] J. Coates, *An effective  $p$ -adic analogue of a theorem of Thue. III. The diophantine equation  $y^2 = x^3 + k$* , *Acta Arith.* **16** (1969/1970), 425–435. MR0263742 (41 #8342)
- [8] J. Cremona, *The elliptic curve database for conductors to 130000*, *Algorithmic Number Theory, Lecture Notes in Comput. Sci.*, vol. 4076, Springer, Berlin, 2006, pp. 11–29, DOI 10.1007/11792086\_2. MR2282912 (2007k:11087)
- [9] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat’s last theorem*, *J. Reine Angew. Math.* **490** (1997), 81–100. MR1468926 (98h:11076)
- [10] J.-H. Evertse, *On equations in  $S$ -units and the Thue-Mahler equation*, *Invent. Math.* **75** (1984), no. 3, 561–584, DOI 10.1007/BF01388644. MR735341 (85f:11048)
- [11] J.-H. Evertse, *The number of solutions of the Thue-Mahler equation*, *J. Reine Angew. Math.* **482** (1997), 121–149, DOI 10.1515/crll.1997.482.121. MR1427659 (97m:11046)
- [12] M. A. Kenku, *On the number of  $\mathbf{Q}$ -isomorphism classes of elliptic curves in each  $\mathbf{Q}$ -isogeny class*, *J. Number Theory* **15** (1982), no. 2, 199–202, DOI 10.1016/0022-314X(82)90025-7. MR675184 (84c:14036)
- [13] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, *Graduate Texts in Mathematics*, vol. 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)
- [14] N. Tzanakis and B. M. M. de Weger, *How to explicitly solve a Thue-Mahler equation*, *Compositio Math.* **84** (1992), no. 3, 223–288. MR1189890 (93k:11025)

CENTER FOR GEOMETRY AND PHYSICS, INSTITUTE FOR BASIC SCIENCE (IBS), 77 CHEONGAM-RO, NAM-GU, POHANG-SI, GYEONGSANGBUK-DO, 790-784, REPUBLIC OF KOREA – AND – POHANG UNIVERSITY OF SCIENCE AND TECHNOLOGY (POSTECH), 77 CHEONGAM-RO, NAM-GU, POHANG-SI, GYEONGSANGBUK-DO, 790-784, REPUBLIC OF KOREA

*Current address:* Department of Mathematics, University of Michigan, 2074 East Hall, Ann Arbor, Michigan 48109-1043

*E-mail address:* dohyeong@umich.edu